Introducing Vigilant Audiences

Daniel Trottier,
Rashid Gabdulhakov
and Qian Huang

https://www.openbookpublishers.com

ISBN Paperback: 978-1-78374-902-7

ISBN Hardback: 978-1-78374-903-4

ISBN Digital (PDF): 978-1-78374-904-1

ISBN Digital ebook (epub): 978-1-78374-905-8

ISBN Digital ebook (mobi): 978-1-78374-906-5

ISBN XML: 978-1-78374-907-2

DOI: 10.11647/OBP.0200

Cover image: Photo by Vino Li on Unsplash at https://unsplash.com/photos/NpYcvUqx8Go

Cover design: Anna Gatti.

Citizens as Aides or Adversaries? Police Responses to Digital Vigilantism

Rianne Dekker and Albert Meijer

Introduction[1]

On social media, citizens are engaging in tasks that traditionally fall within the authority of law enforcement agencies (LEAs). Examples include web-sleuthing collectives solving criminal cases or searching for missing persons (Yardley et al., 2016), specialised networks of paedophile-hunters (Campbell, 2016; Nhan et al., 2017), hacktivist groups revealing cybersecurity breaches or hacking back (E Silva, 2018; Schmidle, 2018) and online neighbourhood-watch schemes (Lub, 2018). Social media has opened up new sources of information about crime to citizens, and it facilitates participation in crime fighting. This includes public denunciation of unwanted behaviour, digital forensics, open source intelligence and crowdsourcing. Cultural norms on social media incite such new forms of civic engagement with public security: social media is non-hierarchical and users have traditionally approached it as a communitarian space governed by libertarian values (Nhan et al., 2017, p. 345).

Online acts of criminal investigation, crime prevention and the denunciation of crime and deviance by citizens, have been gathered

1 The research leading to this chapter has received funding from the European Union's Horizon 2020 Research and Innovation Program, under Grant Agreement no 700281.

 https://doi.org/10.11647/OBP.0200.11

under the labels 'do-it-yourself (DIY) policing' and 'digital vigilantism' (or 'digilantism'). Both concepts refer to citizens performing activities that fall within the discretion of LEAs. At the same time, there is a notable difference between these concepts: DIY policing or digital civilian policing emphasises that it is motivated by a desire to assist law enforcement, for example by analysing available information to identify evidence and suspects (Nhan et al., 2017, p. 347). Usually, DIY police participants collect information on actual or potential crimes and relay this information to law enforcement (Huey et al., 2012, p. 85). In some cases, this is volunteered and in others it occurs in response to official calls for assistance with police work. In contrast, the concept of digital vigilantism stresses the active bypassing of law enforcement and using the public nature of social media for retaliation (Trottier, 2017). Digital vigilantism also includes pursuit and denunciation of a broader set of offences that are immoral rather than illegal. It is characterised by a general perception that law enforcement and the criminal justice system are falling short and different methods of criminal investigation and justice are required (Johnston, 1996; Schuberth, 2013). One could say that the concept of DIY policing highlights the desirable side of participative practices (citizens wanting to contribute to law enforcement efforts), whereas digital vigilantism highlights its negative side (citizens taking public security matters into their own hands).

The concepts of DIY policing and digital vigilantism reflect a normative discussion about the role of citizens in policing, as well as different perceptions the police may hold towards this relatively new type of co-production of public security (cf. Brandsen & Pestoff, 2006). Public security is traditionally governed by the state holding the monopoly on the legitimate use of physical force in a central and hierarchical way, making co-production in this domain disputed. Police responses to different acts of online engagement with public security highlight where normative boundaries between DIY policing and digital vigilantism are drawn. The law enforcement perspective, however, is often missing in research into online engagement with public security. In what cases do the police consider citizens engaged in policing with the support of Web 2.0 as aides or as adversaries? Based on qualitative analysis of round-table discussions among representatives of European law enforcement agencies (LEAs) and other public organisations active in the domain of public security — including local governments, ministries and national

and supranational networks and agencies — this chapter addresses the research question: How do law enforcement authorities decide whether digital contributions of citizens to public security are acceptable?

It is relevant to study law enforcement's stance on the issue because we have seen examples of DIY policing and digital vigilantism in many different countries and even across borders. This study focuses on the perspectives of European law enforcement agencies and reflects upon the generalisability of their views to other police forces worldwide. Furthermore, public debate on the desirability of online citizen engagement with public security is growing. As authorities in the domain of public security, LEAs are in a position to informally and formally encourage or discourage various acts of online engagement with public security. According to Huey et al. (2012, p. 95) "continued efforts should be made to understand further police attitudes towards these groups and how more fruitful co-operative relations could be developed".

By studying the perceptions of LEAs we also contribute to a theoretical understanding of which new patterns of co-production between law enforcement agencies and (collectives of) citizens are developing in an information age. Public administration literature claims that social media is strengthening co-production (Linders, 2012; Meijer, 2012). This chapter develops a typology to come to a more fine-grained understanding of the manifold forms of online co-production of public security, and discusses several ways to guide desirable and undesirable practices.

Online Co-Production of Public Security

Over the past decades, governments have moved from providing public services themselves to increasingly involving civil-society actors and citizens in the provision of public services. Public administration studies of co-production describe examples in healthcare, social welfare, community services and other public domains (Brandsen & Pestoff, 2006; Voorberg et al., 2015). Co-production has also made its way into the domain of public security, with strategies of plural policing and community policing. The concept of plural policing relates to how responsibilities for policing and security services extend from sovereign states to private companies, transnational arrangements and

citizens (Loader, 2000; O'Neill & Fyfe, 2017). Community policing has emerged as a police operating paradigm of close collaboration with citizens to maintain public security. Community policing entails informing and engaging citizens as experts within their local context, and being responsive to their information and requests (Mastrofski et al., 1995; Skogan & Williamson, 2008). In these policing strategies, non-state actors and citizens are not only 'clients' of the police, but also active contributors to the production of public security (Percy, 1978). Consequently, modern sovereign states no longer have a monopoly on the use of legitimate force within given spatial boundaries.

The platforms of Web 2.0 are strengthening collaboration with citizens in various public domains, including public security (Linders, 2012). They facilitate sharing and discussion of user-generated content within communities of interest (Haythornthwaite, 2005, p. 140) and enables a direct connection with government (Frissen et al., 2008). Meijer (2012, p. 1158) outlines how new media are an important facilitator for new forms of co-production, because the costs of connecting to citizens have been reduced drastically and the new technologies create opportunities to interact 24/7. The Citizen's Net (*Burgernet*) application (app) — one of the cases in this study — enables the Dutch police to send out a digital message to call upon the help of citizens within a specific geographical area. It enables citizens to participate in solving local crime or missing-persons cases in the 'golden hour' directly after the incident. Citizens can respond with their information and receive a message when the situation is solved and their information is no longer requested. Such instantaneous, rich and synchronous forms of interaction between citizens and government can hardly be created without the networked infrastructure provided by social media.

Linders (2012) proposes a typology of co-production supported by social media in which collaboration between government and citizens can take different forms. He distinguishes "government as a platform", "citizen sourcing" and "do-it-yourself government" (ibid., p. 447). In government as a platform, the initiative for co-production lies with government, reaching out to citizens for specific forms of input. The "Citizen's Net" (*Burgernet*) app from the Dutch police would be an example of this (cf. Meijer, 2012; 2015). In citizen sourcing, the initiative for co-production lies with citizens. The public helps government

to be more responsive and effective, for example, by reporting local disturbances to the police. Government holds the primary responsibility for action, but citizens influence the direction and outcomes, improve the government's situational awareness, and may even help to execute government services on a day-to-day basis. Already, in these government-led types of digitally supported co-production, we see the risk of citizens infringing upon each other's privacy, and the risk of citizens taking vigilante actions. Participation is sometimes motivated by entertainment and a notion of gaming, besides or instead of a motive of civic responsibility (Meijer, 2012, p. 1168): "Intervening in police work turns into a real life game in which everybody can participate. Get a text message, look out of your window, and catch the thief". Excitement about participation in police work can become problematic when it turns into a competition between citizens, and this might encourage unethical or even illegal behaviour in order to solve crime.

These risks become even greater when online co-production is not initiated by, or does not occur in close collaboration with government. Do-it-yourself policing and digital vigilantism would fall into the category of 'do-it-yourself government'. Social media has opened up opportunities for this type of citizen-to-citizen co-production of public security. This poses larger risks to government than online forms of co-production that are initiated and closely coordinated by government (Linders, 2012). While possibly being very effective and low-cost for government, communities of interest engaged with this form of co-production may step out of line. How is this 'line' defined by government actors in the domain of public security? And how does this distinction generate different police responses that are intended to fit online co-production within their standards of fruitful cooperation? These questions, which are still unanswered in public administration literature, will be addressed in this chapter.

Method

Data on attitudes and responses towards online co-production of public security were collected in round-table discussions amongst public security practitioners. Six European practitioner workshops on various topics related to DIY policing and digital vigilantism were

organised over the course of 2017 and 2018 in the context of the Horizon 2020 project Medi@4Sec (www.media4sec.eu). The topics of these workshops were: DIY Policing, Riots & Mass Gatherings; the Dark Web; Everyday Policing; Trolling; and Innovative Market Solutions. A variety of practitioners from European LEAs and other organisations active in the domain of public security were invited, based on their experience with the workshop themes. This included representatives of local and national police forces, police colleges and police networks, but also representatives from local, regional and national governments, NGOs, private companies and research institutes (Table 11.1). Practitioners came from various Northern, Southern, Central and Eastern European countries, but representatives from countries that were more actively engaging with social media — such as the UK and the Netherlands — were overrepresented (Figure 11.1). The numbers of workshop participants ranged between 30–40 for each workshop, creating a total of 215 workshop participants. This total includes approximately 30 participants who attended multiple workshops, so the total of unique participants is around 150.

The round-table discussions were led according to the World Café format. This format entails collaborative group dialogues wherein knowledge is gathered and shared amongst practitioners. It stimulates thinking about *current* and *ideal* practices by creating an informal sphere of discussion (Stewart, 2005; Fouché & Light, 2011). The goal of the round-table discussions in the World Café format was to formulate recommendations and action points for public security actors. Discussions at each table included between four and six practitioners and took 30 to 45 minutes per round table, before participants moved on to a second round table with a different composition of practitioners. Each practitioner participated in two round-table discussions per workshop. Two 'table hosts' from the project consortium moderated the discussions and took notes. After a short round of introduction, the main questions leading the debate in each of the workshops were: In what ways have you/has your organisation encountered this phenomenon? What are current practices? How could these be improved into ideal practices? The round-table discussions took place under Chatham House rules, creating an open discussion. Table hosts summarised the discussion on paper and publicly presented the main outcomes to the workshop participants to collect final questions and feedback.

Table 11.1: Sectors represented by workshop participants

Sector	**N**
Police	109
Research	28
Private sector	24
Local government	18
Regional/national government	21
NGO	13
Other	2
Total	215

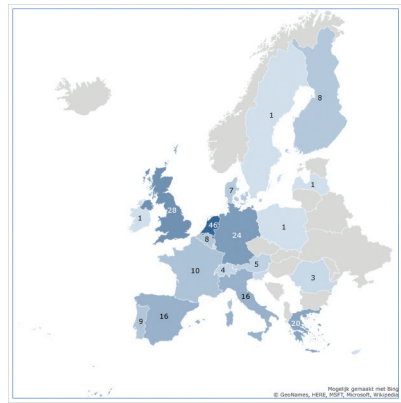

Fig. 11.1 Countries represented by workshop participants (Total N=215) *Three private-sector delegates represented organisations from the United States.

For the research aims of this chapter, anonymised summaries of the round-table discussions were qualitatively coded. This entailed a process of open coding in dialogue with the focus of the research question. We coded (1) various forms of online citizen co-production of public security that are distinguished by law enforcement authorities; (2) the response they received; and (3) whether they are deemed acceptable or unacceptable and why. This explorative analysis provides an image of which acts of online co-production of public security are considered to be helpful or disruptive by law enforcement authorities

in Europe, and how they are therefore met with different responses. It reveals how police professionals discursively construct citizens as aides or adversaries.

A limitation of our method is that the workshops and round tables each focused on a distinctive topic, such as 'DIY Policing' and 'Everyday policing' (with a more positive connotation) or 'trolling' (with a negative connotation). This influenced the tone of the discussion, but still left space for different interpretations and opinions — as the data show. Because the round-table discussions took place under Chatham House rules, our analysis was based on anonymised summaries of the discussions and we were unable to link statements to specific actors, nor could we distinguish whether statements were broadly supported by different actors. The summaries represent the majority views and the data are presented as general opinions. This means that we refrain from making statements on the prevalence of views and only use direct quotes when these were very strongly voiced and stressed in the summary reports.

Results

Online co-production of public security is responded to in various ways by practitioners, highlighting different attitudes towards different forms of engagement. The sections below outline which acts of online engagement are considered helpful and which are considered disruptive by LEAs and other public security actors. Based on analysis of practitioner dialogues, we interpret where these discursive boundaries are drawn by focusing on specific policing tasks and images of the citizens involved.

Accepted Forms of Online Co-Production of Public Security

Online acts of denouncing crime are generally evaluated positively by public security practitioners. Sometimes denunciation happens implicitly when criminal acts are shamed or mocked, and sometimes this is done directly when citizens discipline the behaviour of others on social media. This type of online engagement is generally considered as a helpful form of crime prevention. Public security actors expect it to

create enhanced awareness of the rule of law and to reinforce societal norms of accepted behaviour and deviance. Discussions during the trolling and DIY policing workshops highlighted that this form of engagement in crime prevention is seen as a positive contribution to police efforts.

More institutionalised forms of participation in crime prevention are also welcomed. For example, when citizens are sharing police warnings through social media — as discussed in the Everyday Policing workshop. This is expected to raise citizens' overall awareness of public security risks and to enable them to deal with minor issues amongst themselves before they escalate to a level requiring police intervention. This more formal and government-led form of engagement and collaboration in crime prevention is expected to enhance citizens' trust in the police as a modern, professional and open organisation, and to reinforce good relations between police and the public. The Innovative Market Solutions workshop indicates that several European police forces are using, acquiring or developing online tools or apps to encourage participation in crime prevention.

Other acts of online policing, besides engagement with crime prevention, are seen as more risky, but are generally valued when they resemble offline forms of collaboration with police. Two aspects mentioned during the DIY policing workshop are key in distinguishing these types of acts as helpful: first, collaborating with the police by, for example, bringing tips on cases, evidence or suspects to the police. Citizens doing this are seen as aides when they share the objectives of public security actors and are collaborating within their professional standards. A second aspect based on which practitioners distinguish this behaviour as acceptable is when online co-production focuses on cases directly affecting citizens' own neighbourhoods or communities. When citizens are former or potential victims and have a legitimate concern for their personal safety, public security practitioners are understanding of their engagement and involvement. Both aspects reflect the ideal of community policing.

Online co-production in activities that go beyond this operating philosophy of community policing are approached more reluctantly. Online open source investigations by the Bellingcat collective and by citizens after the Boston Marathon bombings were referenced during

the DIY policing workshop as prominent examples of this. Their actions were considered as risky, since they led to premature accusations and interference with ongoing operations. However, several practitioners in the DIY Policing, Riots and Mass Gatherings and Everyday Policing workshops noted that citizens engaging in these types of online co-production of safety were also sometimes aiding police work. They can act as additional 'eyes and ears' of the police when they are investigating large amounts of evidence using their own expertise and professionalism (cf. Nhan et al., 2017). Collectives engaged in investigating crimes and public disorder are seen as having a broad range of skills, which can provide interesting new leads. Also, citizens policing the social spaces of Web 2.0 — for example in tracing illegal activity on the Dark Web — are considered helpful. Many public security practitioners see their organisations as under-resourced, which prevents them from having a meaningful presence online (Dark web workshop; cf. Huey et al., 2012). Online engagement with crime and deviance beyond citizens' own locality is approached with caution, but some practitioners note that it is only logical that social media are pushing the boundaries of the locally-based model of community policing towards matters outside of citizens' own communities and towards the online space (DIY Policing workshop).

Unacceptable Forms of Online Co-Production of Public Security

Forms of online co-production that go beyond collaboration with LEAs within the citizens' local context are generally deemed disruptive. Public security actors in the DIY Trolling workshops expressed two main concerns: these forms of online co-production can be harmful to other citizens and society and they can be harmful to the efforts of law enforcement.

Harm to Citizens and Society

Three arguments were presented about why online co-production can be harmful to citizens and society: Firstly, online co-production is seen as harmful to other citizens and society when *premature accusations that*

other citizens are criminal offenders are voiced online. Online collaboration can give way to rampant speculation, including the mislabelling of innocent actions as suspicious activities and the misidentification of innocent individuals as legitimate suspects (cf. Nhan et al., 2017, p. 353). This may happen, for example, in online neighbourhood-watch groups (DIY Policing workshop). Online manhunts are most harmful when they concern innocent suspects, but even when speculations in the end turn out to be correct, some public security practitioners see this as harmful to the suspect and prosecution of the case. Using online naming and shaming as a means of reprisal brings unnecessary harm to the suspect, and it is not usually possible for the suspect to be forgotten by having all online material deleted after sentencing is completed (cf. Kohm, 2009; Mayer-Schönberger, 2009). DIY Policing and Trolling workshop participants noted that the public shaming of suspects can lower the sentencing in court. Here, practitioners distinguish acts of naming and shaming as a way of crime prevention and retaliation. It is only accepted when its main purpose is warning others not to engage in or not to become a victim of this kind of behaviour.

Secondly, it was argued that online engagement with public security may *focus only on effectiveness and not on process values*. It was mentioned in the DIY Policing workshop that individuals and collectives who are engaged with public security mainly strive for effectiveness, and that this is the only measure on which they grade their success. They aim for quick and high numbers of apprehensions. However, they do not adhere to other public values that enable due process in criminal investigations (cf. Jørgensen & Bozeman, 2007; De Graaf & Meijer, 2019). The values that were mentioned as lacking include the protection of data and privacy, necessity and proportionality, non-discrimination and accountability for one's actions. Decisions about who to punish and how to do this are not transparent, accountable or democratically legitimate in such cases. In this respect, the authority of online crime fighters is highly questionable, even when their targets are quite obviously engaged in criminal behaviour (cf. Rizza et al., 2012). Also, citizens' measurement of effectiveness was critically discussed in the DIY Policing workshop. It was stated that digital vigilante groups often target 'low-hanging fruits' that are easily caught but are also causing relatively little harm. Apprehending more professional offenders requires more elaborate

investigation, which takes time, and apprehension rates might thus be lower. However, when measured in years of sentencing instead of numbers of apprehensions, police cases can be seen as more successful.

Another related concern of public security practitioners is when individuals or groups engage in *unprofessional practices of criminal investigation and punishment* (DIY Policing workshop; cf. Huey et al. 2012). Acts that are clearly labelled in the DIY Policing and Trolling workshops as 'vigilante' include entrapment, for example by acting as a decoy to uncover paedophiles, infiltrating websites and organisations, illegitimate ways of collecting evidence (for example the use of drone images) and doxing (Trolling workshop). The latter entails acts of harvesting and publishing private information about a particular individual online (cf. Trottier, 2017). This is seen as not only harmful to suspects, but possibly also to the digital vigilantes themselves when they are dealing with dangerous suspects. They can become a victim of criminals who feel threatened by digital vigilantes.

Harm to Police Operations

Practitioners also identified several dangers to police work of online co-production of public security. Again, three arguments were provided. First, practitioners on a local and national level voiced a very practical concern that an abundance of online engagement can *overburden police with information and demands for intervention* (Everyday Policing workshop). These demands might not always be met in case of petty incidents, because the police have to prioritise due to limited resources (cf. Nhan et al., 2017). When the police become more easily approachable through its social media presence or specialised apps, practitioners expect that the threshold to seek the help of law enforcement will become lower (DIY Policing workshop). Particularly, practitioners fear a growing number of requests related to offenses in cyberspace such as trolling, cyber-bullying and online shaming. However, much of this is not illegal and is dealt with most easily by moderation implemented by social media platforms, or solved by citizens amongst themselves (Trolling workshop). The presence on social media of police and police apps raises the expectation that all notifications will be dealt with. If

this expectation is unfulfilled, that might undermine trust in police and encourage vigilante acts.

Practitioners are also concerned that online engagement with crime may *jeopardise ongoing police investigations and criminal prosecution of cases*. Citizens can, for example, resort to unlawful acts to collect evidence, tamper with evidence or publish information online that is kept classified in a police investigation (DIY Policing workshop). Public anti-authoritarianism — which is typical to some online platforms — coupled with a personal sense of right and wrong, often conflicts with legal standards and complicates police efforts. In response, we learned during the Innovative Market Solutions workshop that LEAs are using data mining and analysis tools to keep track of online engagement with ongoing police investigations (cf. Žitnik et al., 2018). This helps identify information that might distort the investigation, such as incorrect information that causes panic or leads to harmful actions. Information from online sources may also bring new leads for the investigation. Some practitioners, however, note that online publics only rarely bring new information to the table and often cause more harm than benefit (DIY Policing workshop; cf. Huey et al., 2012). According to these practitioners, the expertise and successes of digital vigilante groups are exaggerated by the groups themselves and in news reports of their activities.

Relatedly, there is a concern that online co-production of public security *undermines police authority*. When stories of successful apprehensions are uncritically shared and picked up by news media, and when there is no accountability or transparency about the actions that did not lead to success, public security practitioners are concerned that this may undermine trust in the police and eventually police authority and legitimacy (DIY Policing workshop). An example that was discussed during the DIY workshop was that of online paedophile-hunter groups. In an increasing number of grooming trials, evidence from these groups is used. The groups are actively listing successful apprehensions and convictions on their websites.[2] When the police are seen as ineffective and inefficient, citizens may increasingly resort to taking matters into their own hands — with the risk that their

2 See for example www.darkjustice.co.uk.

unprofessionalism has negative consequences, as well as the lack of due process to other citizens and society outline above.

Discussion: Online Citizens as Aides and Adversaries

Our analysis of discussions amongst European practitioners about online co-production in public security reveals that discursive boundaries of helpful and harmful acts of are not only drawn based on involvement in specific police tasks, such as crime prevention vs. investigation and prosecution. Discursive boundaries are primarily drawn based on the resemblance with the existing operating paradigm of community policing (Mastrofski et al., 1995; Skogan & Williamson, 2008). While there are many differences between countries in adopting this policing paradigm, among Northern and Western European countries it has become relatively popular. Countries that are more democratically consolidated tend to have stronger relative preferences towards community-oriented policing over zero-tolerance styles (Lum, 2009). Distinctions between DIY policing and digital vigilantism by public security practitioners in these countries are based on this model.

Citizens are considered as aides to police efforts when they engage with cases relating to their local context and when they closely collaborate with law enforcement. When online engagement goes beyond this familiar model of co-production, citizens are more likely to be considered adversaries. This concerns involvement in cases outside of citizens' own local contexts and when they do not collaborate with law enforcement, or when they do so only at a later stage in order to be able to claim their own successes. These groups are seeking a broader audience in order to publicly denounce and retaliate against crime, instead of wanting to solve issues locally within the criminal justice system. From the perspective of public security actors, this is what distinguishes harmful digital vigilantism from helpful DIY policing.

Based on these two distinguishing features of DIY policing and digital vigilantism, we can develop a more fine-grained typology of online co-production in the domain of public security, including examples of behaviours that were brought up in the discussions (Table 11.2).

Table 11.2: Typology of online civic engagement in public security

	Cases within citizen's local context	**Cases outside of citizen's local context**
Close collaboration with law enforcement	Discussing tips on suspects or missing persons based on evidence posted by police on social media	Investigating evidence from social media sources on rioters, hooligans or terrorists and bringing this to the police
Late or no collaboration with law enforcement	Neighbourhood watch groups working independently from local police, bringing offenders to justice themselves	Online entrapment of offenders and bringing these cases to the police only afterwards, hacking or phishing and doxing suspects without bringing these cases to the police

Public security organisations in various European countries are at different stages of maturity in responding to these various types of online co-production. This depends on the technological resources of the police force, the political context of the country and the local police culture. Presumably, the differences with countries beyond the EU are even larger. Police forces with less financial and technological resources, within authoritarian political systems and with a repressive police culture will engage less in co-production of public security with online citizens. Representatives from European LEAs who participated in our workshop share a similar ideal of better engaging with DIY policing and more strongly denouncing digital vigilantism.

Two ideal typical forms of DIY policing and digital vigilantism are highlighted in the upper-left and lower-right boxes of Table 11.2. There is consensus that local, collaborative forms of engagement with public security, such as sharing and discussing tips on suspects or missing persons based on evidence posted by police on social media, should be better facilitated and encouraged. Some police forces are already doing so by hosting various social media channels on which calls to action are posted, or having specialised apps to ask for collaboration in local cases. Examples are Amber Alert and the Dutch 'Citizen's Net' app (cf. Meijer, 2012; 2015). More common are police forces that only

host one centralised social media account, which is used to disseminate information to the public and not to interact with the public. This type of social media adoption reinforces a traditional and hierarchical model of the police as knowledge broker (Nhan et al., 2017, p. 344).

There is also relative consensus that ideal typical forms of digital vigilantism — as highlighted in the lower-right box of Table 11.2 — should be more strongly denounced by LEAs. Even though, in some cases, the specific expertise and resources of online publics are valued, the police consider the independence with which these groups are working and claiming successes as harmful to society and to police authority. Public security actors fear that only the positive successes of these individuals and collectives are celebrated, while the many compromises that are made with regard to public values other than effectiveness, such as the privacy of suspects, are too easily ignored. While harmful acts towards others, such as trolling and doxing, may be unethical but not illegal, some public security actors wish to pursue current regulations more strictly, or to expand them. Other public security actors wish to publicly counter the successes of digital vigilantes by providing information on negative side-effects and offering a counter-narrative.

Literature on digital vigilantism suggests that these forms of guidance would have limited effects. Since social media spaces are governed by libertarian and sometimes anti-authoritarian values, online publics will not always self-identify as vigilante or be willing to follow the procedures of law enforcement. Also, because social media spans national borders, citizens engaging in DIY policing will belong to multiple jurisdictions that may have different guidelines. As stated earlier, countries with more authoritarian governance systems are not likely to have a tradition of community policing or to employ a positive stance towards the online engagement of citizens in police work. In these cases, police attitudes towards citizens prevent them from taking online co-production seriously. There is a police subculture of distrust, in which citizens are stereotyped either as "know nothings", "suspicious persons" or "assholes" (Manning & Van Maanen, 1978, pp. 223–4). This mutual distrust might be reinforced by the anonymity of social media (Walker et al., 2006) and will complicate attempted collaboration in online spaces.

The two forms of online civic engagement that were debated more intensively are found in the upper-right and lower-left boxes of Table 11.2. Public security actors see some merit in both, but are also concerned with their negative effects. When collaborative engagement occurs outside citizens' local contexts, their level of expertise was debated. Are they able to bring new leads to the table that the police investigation would not have uncovered? Some practitioners pointed towards strained police resources and the "wisdom of the crowds" (cf. Surowiecki, 2004) that online citizens can contribute to the investigation. Besides this crowdsourcing of intelligence, others value the specific expertise of some citizens in more specialised investigations, such as cybercrime. The motives of citizens to help in cases outside of their own communities are questioned, however. Why would citizens offer their time and skills to collaborate with law enforcement when they have no direct fear for their own safety, or for that of others within their community? Some practitioners fear that the desire to match or outsmart law enforcement will lead these citizens to take bold measures, and to lose sight of public values that are equally as important as effectiveness.

Meijer (2012) describes how online co-production in the domain of public security can indeed be motivated by entertainment, or even have an element of 'gaming' to it. However, in this digital age, engagement with criminal cases outside of one's local context can also be motivated by local concerns and a sense of civic responsibility. In her seminal book *The Death of Distance* (1997) Cairncross claims that the revolution in telecommunications technologies makes geographical distance less significant. Studies on the effects of Web 2.0 also note how social media makes geographical borders less relevant. However, other borders remain present: for example, language barriers preventing people from communicating with each other, and social borders distinguishing cases which *feel* familiar enough to engage with. Due to the media-rich and personal nature of social media communication, citizens can feel closely engaged with cases from which they are geographically far removed. This may motivate them to contribute digitally to policing efforts.

In the case of online engagement with local cases without collaboration with the police, citizens' own methods of seeking justice are problematised most. Engagement with local issues of public security is valued. However, it is exactly because matters are close to home, that

public security actors fear it is tempting for citizens to take matters into their own hands. For example, neighbourhood watch groups may use their online platforms to encourage people to bring suspects to justice themselves. When collaboration with the police is not sought, or is sought only at a late stage, practitioners fear that methods of investigation and punishment are unlawful, unprofessional and cause harm to suspects, to other citizens, and to social cohesion in local communities. European police forces are developing apps to facilitate engagement in prevention and investigation, according to law enforcement standards. For example, the police in Nice (France) piloted the app C-Now (previously Reporty) in which citizens can take videos of incidents and crime and live-share this information, including geolocation, with emergency operators. The Dutch police is developing apps to engage citizens in finding missing persons (*Samen zoeken*) and securing evidence after a crime (Sherlock).

Conclusions

Online forms of co-production of public security are here to stay, but the rules of this 'game' have yet to be established. DIY policing and digital vigilantism can be considered as examples of "do-it-yourself government" (cf. Linders, 2012). These forms of online co-production are initiated by citizens, take place relatively independently of government law enforcement, and are therefore most ambiguous. As authoritative actors within the domain of public security, law enforcement agencies and other public organisations involved with public security play an important role in establishing the boundaries between acceptable and unacceptable forms of online engagement. In their responses to different forms of online civic engagement, they discursively set these boundaries. This chapter has therefore addressed the question of how law enforcement authorities define the boundaries of which digital contributions of citizens to public security are acceptable, and which unacceptable.

An analysis of round-table discussions between European public security practitioners, during six workshops, highlights that discursive boundaries of accepted forms of online co-production are drawn based on the existing philosophy of 'community policing'. In this policing-operation paradigm, engagement is characterised by close collaboration

with law enforcement and involvement in cases concerning citizens' local communities. Acts of online engagement with matters of public security that fall outside of this definition — either on one or on both conditions — are met with more skepticism and reluctance. They are considered to bring risks of harm to others in society, as well as to police work and police authority.

Broad definitions of DIY policing and digital vigilantism generate only limited understanding of the different responses of LEAs towards online civic engagement. Developing a more fine-grained distinction and typology based on these two key features of community policing is helpful to understanding normative boundaries drawn by authorities, and probably also by less authoritative actors towards this phenomenon. As authorities in the domain of public security, LEAs and local, national and international public security organisations are in a position to formally and informally define the boundaries of accepted acts of DIY policing, which will probably also permeate to less authoritative actors and citizens (cf. Schneider, 2014).

Our research details shared perceptions of LEAs in Europe regarding online engagement of citizens in security practices. It provides important insights in what is seen as acceptable and unacceptable behaviour on the Internet. Unfortunately, based on the anonymous character of the round-table discussions and reporting, we were not able to distinguish differences in opinion between LEAs in different European countries or between actors working for different types of public security organisations. This raises a set of new questions. Further research should focus on investigating the similarities and differences between countries with different political contexts and police cultures. Comparative research enables us to understand how national security cultures translate into police engagement with online co-production of public security. In addition, we need to investigate the actual responses of the police to find out whether their actions indeed fit the matrix that we developed based on their statements. Are they indeed more supportive of local practices and practices in close collaboration with law enforcement?

The research maps current views but also raises questions about the future. Police notions of what is a 'local context' and 'close collaboration' — the two key dimensions in our model — may start to

shift and change. Local context used to be defined in a geographical sense, but this is shifting with the death of distance and it may require a new meaning in the "space of flows" (Castells, 1999, p. 294). Citizens might feel close affinity with others in different localities, which motivates them to engage with their public security issues. Furthermore, close collaboration was previously defined as following police orders: government-as-a-platform forms of co-production. Now, this may become a more horizontal collaboration. These shifts will define what LEAs see as acceptable and unacceptable forms of online citizen engagement and what they label as DIY policing and digital vigilantism.

For some European law-enforcement authorities, it has been difficult to diverge from their traditional authoritative role as knowledge brokers, and instead to actively engage with social media to guide the online activities of citizens. They generally feel that there is little that they can do to stop new forms of online engagement with public security and it is also not in their best interest to do so. Therefore, we observed a shared desire amongst the group of public security practitioners to provide more guidance in online civic engagement with policing. By stonewalling or denouncing all types of online citizen engagement, LEAs would miss out on an opportunity to acknowledge legitimate concerns for public security, with the risk that citizens might lose trust in the police, causing the erosion of police legitimacy (cf. Crump 2011; Meijer & Thaens 2013; Warren et al. 2014; Grimmelikhuijsen & Meijer 2015). They feel that judgements on these co-production initiatives should not be left only to online collectives themselves, or to the public courts of news media and public opinion.

Several options to provide more guidance, including regulations, training, moderation and apps were proposed. They are mostly proposed within the traditional domains of community policing such as crime prevention, tracing missing persons and addressing local nuisance, disorder and petty crimes. In more specialised disciplines and larger cases such as white-collar crime, sexual assault and murder cases, online civic engagement is generally deemed less suitable and guidance was not proposed in order not to inadvertently encourage involvement. Public security actors wish to direct online publics to key areas of investigation and help focus their efforts. Furthermore, police guidance

would help to ensure transparency in evidence collection and study, and it is expected to steer citizens towards more professional norms.

Many acts of digital vigilantism cannot be forbidden as being unlawful, but are simply unethical. In the case of unlawful acts, it is doubtful whether public security actors will achieve the desired goal of guiding digital vigilantes towards DIY policing characterised by close collaboration with law enforcement and involvement in only local matters. Digital vigilantes might not self-identify as such, and even if they do, their vigilante acts might be an active choice based on anti-authoritarianism and distrust in government law enforcement. At the same time, providing more guidance to those engaged in DIY policing may come at a price. It can create an implicit incentive for citizens to get (more) involved in matters of public security, although this has not been the primary goal: public security actors only wished to guide existing involvement, as an overabundance of tips and requests is already a concern. Coordinating DIY policing activities may also create new liabilities for the police when acts by citizens that have been coordinated by the police cause harm after all (cf. Huey et al., 2012). Lastly, facilitating online involvement in public security can stimulate an atmosphere of social control and mutual distrust amongst citizens (cf. Schreurs et al., 2018). Existing social, cultural and political divides in society might become more prominent. These matters should be taken into account by public security actors when providing more guidance to DIY policing.

References

Bekkers, V. J. J. M., & Meijer, A. J. (2010). *Co-creatie in de publieke sector; Een verkennend onderzoek naar nieuwe digitale verbindingen tussen overheid en burger*. Den Haag: Boom Juridische Uitgevers.

Brandsen, T., & Pestoff, V. (2006). Co-production, the third sector and the delivery of public services: An introduction. *Public Management Review,* 8(4), 493–501, https://doi.org/10.1080/14719030601022874

Cairncross, F. (1997). *The Death of Distance: How the Communications Revolution Will Change our Lives*. Brighton: Harvard Business School Press.

Campbell, E. (2016). Policing paedophilia: Assembling bodies, spaces and things. *Crime, Media, Culture,* 12(3), 345–65, https://doi.org/10.1177/1741659015623598

Castells, M. (1999). Grassrooting the space of flows. *Urban Geography,* 20(4), 294–302, https://doi.org/10.2747/0272-3638.20.4.294

Crump, J. (2011). What are the police doing on Twitter? Social media, the police and the public. *Policy & Internet*, 3(4), 1–27, https://doi.org/10.2202/1944-2866.1130

De Graaf, G., & Meijer, A. (2019). Social media and value conflicts: An explorative study of the Dutch police. *Public Administration Review,* 79(1), 82–92, https://doi.org/10.1111/puar.12914

E Silva, K. K. (2018). Vigilantism and cooperative criminal justice: is there a place for cybersecurity vigilantes in cybercrime fighting? *International Review of Law, Computers & Technology,* 32(1), 21–36, https://doi.org/10.1080/13600869.2018.1418142

Fouché, C., & Light, G. (2011). An invitation to dialogue: The World Café in social work. *Qualitative Social Work,* 10(1), 28–48, https://doi.org/10.1177/1473325010376016

Frissen, V., Van Staden, M., Huijboom, N., Kotterink, B., Huveneers, S., Kuipers, M., & Bodea, G. (2008). *Naar een 'User Generated State'? De impact van nieuwe media voor overheid en openbaar bestuur*. Report for the Dutch Department for the Interior, The Hague.

Grimmelikhuijsen, S. G., & Meijer, A. J. (2015). Does Twitter increase perceived police legitimacy? *Public Administration Review,* 75(4), 598–607, https://doi.org/10.1111/puar.12378

Haythornthwaite, C. (2005). Social networks and internet connectivity effects. *Information, Communication & Society,* 8(2), 125–47, https://doi.org/10.1080/13691180500146185

Huey, L., Nhan, J., & Broll, R. (2012). 'Uppity civilians' and 'cyber-vigilantes': The role of the general public in policing cyber-crime. *Criminology and Criminal Justice,* 13(1), 81–97, https://doi.org/10.1177/1748895812448086

Johnston, L. (1996). What is Vigilantism? *British Journal of Criminology,* 36(2): 220–36, https://doi.org/10.1093/oxfordjournals.bjc.a014083

Jørgensen, T. B., & Bozeman, B. (2007). Public values: An inventory. *Administration & Society,* 39(3), 354–81, https://doi.org/10.1177/0095399707300703

Kohm, S. A. (2009). Naming, shaming, and criminal justice: Mass-mediated humiliation as entertainment and punishment. *Crime, Media, Culture,* 5(2), 188–205, https://doi.org/10.1177/1741659009335724

Leach, P. (2003). Citizen Policing as Civic Activism: An International Inquiry. *International Journal of the Sociology of Law,* 31(3), 267–94, https://doi.org/10.1016/j.ijsl.2003.09.006

Linders, D. (2012). From e-government to we-government: Defining a typology for citizen coproduction in the age of social media. *Government Information Quarterly,* 29(4), 446–54, https://doi.org/10.1016/j.giq.2012.06.003

Loader, I. (2000). Plural Policing and Democratic Governance. *Social and Legal Studies,* 9(3), 323–45, https://doi.org/10.1177/096466390000900301

Loveluck, B. (2016). Digital vigilantism, between denunciation and punitive action. *Politix,* 115(3), 127–53, https://doi.org/10.3917/pox.115.0127

Lub, V. (2018). *Neighbourhood Watch in a Digital Age. Between Crime Control and Culture of Control.* Cham: Palgrave McMillan, https://doi.org/10.1007/978-3-319-67747-7

Lum, C. (2009). Community policing or zero tolerance? Preferences of police officers from 22 countries in transition. *The British Journal of Criminology,* 49(6), 788–809, https://doi.org/10.1093/bjc/azp039

Manning, P., & Van Maanen, J. (1978). *Policing: A View from the Street*. Santa Monica, CA: Goodyear.

Mastrofski, S. D., Worden, R. E., & Snipes, J. B. (1995). Law enforcement in a time of community policing. *Criminology,* 33(4), 539–63, https://doi.org/10.1111/j.1745-9125.1995.tb01189.x

Mayer-Schönberger, V. (2009). *Delete: The Virtue of Forgetting in the Digital Age.* Princeton University Press, https://doi.org/10.1515/9781400838455

Meijer, A. J. (2012). Co-production in an information age: Individual and community engagement supported by new media. *VOLUNTAS: International Journal of Voluntary and Nonprofit Organizations,* 23(4), 1156–72, https://doi.org/10.1007/s11266-012-9311-z

Meijer, A. J. (2015). E-governance innovation: Barriers and strategies. *Government Information Quarterly,* 32(2), 198–206, https://doi.org/10.1016/j.giq.2015.01.001

Meijer, A. J., & Thaens, M. (2013). Social media strategies: Understanding the differences between North American police departments. *Government Information Quarterly,* 30(4), 343–50, https://doi.org/10.1016/j.giq.2013.05.023

Nhan, J., Huey, L., & Broll, R. (2017). Digilantism: An analysis of crowdsourcing and the Boston marathon bombings. *The British Journal of Criminology,* 57(2), 341–61, https://doi.org/10.1093/bjc/azv118

O'Neill, M., & Fyfe, N. R. (2017). Plural policing in Europe: relationships and governance in contemporary security systems. *Policing and Society,* 27(1), 1–5, https://doi.org/10.1080/10439463.2016.1220554

Percy, S. L. (1978). Conceptualizing and Measuring Citizen Co-Production of Community Safety. *Policy Studies Journal,* 7, 486–93, https://doi.org/10.1111/j.1541-0072.1978.tb01797.x

Rizza, C., Pereira, Â. G., & Curvelo, P. (2014). "Do-it-yourself justice": Considerations of social media use in a crisis situation: The case of the 2011 Vancouver riots. *International Journal of Information Systems for Crisis Response and Management* (*IJISCRAM*), 6(4), 411–15, https://doi.org/10.4018/ijiscram.2014100104

Schmidle, N. (2018, May 7). The digital vigilantes who hack back. *The New Yorker Magazine*, https://www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back

Schneider, C. J. (2014). Police 'image work' in an era of social media: YouTube and the 2007 Montebello summit protest. In Trottier, D. & Fuchs, C. (eds). *Social Media, Politics and the State: Protests, Revolutions, Riots, Crime and Policing in the Age of Facebook, Twitter and Youtube* (pp. 227–46). New York: Routledge, https://doi.org/10.4324/9781315764832

Schreurs, W., Kerstholt, J. H., de Vries, P. W., & Giebels, E. (2018). Citizen participation in the police domain: The role of citizens' attitude and morality. *Journal of Community Psychology,* 46(6), 775–89, https://doi.org/10.1002/jcop.21972

Schuberth, M. (2013). Challenging the weak states hypothesis: vigilantism in South Africa and Brazil. *Journal of Peace, Conflict & Development*, 20, 38–51.

Skogan, W. G., & Williamson, T. (2008). An overview of community policing: origins, concepts and implementation. In: Williamson, T. (ed.) *The Handbook of Knowledge-Based Policing: Current Conceptions and Future Directions* (pp. 43–58) Chichester: John Wiley & Soons, https://doi.org/10.1002/9780470773215.ch1

Smit, P. H. (2017, October 10). Dankzij deze apps kan iedereen straks meespeuren met de politie. *de Volkskrant*, https://www.volkskrant.nl/binnenland/dankzij-deze-apps-kan-iedereen-straks-meespeuren-met-de-politie~a4520905

Stewart, A. (2005). On conversation and collective questioning: theory and practice of the World Café. *System Thinker,* 16(5), 9–10.

Surowiecki, J. (2004). *The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies and Nations*. New York: Doubleday.

Trottier, D. (2017). Digital vigilantism as weaponisation of visibility. *Philosophy & Technology,* 30(1), 55–72, https://doi.org/10.1007/s13347-016-0216-4

Voorberg, W. H., Bekkers, V. J. J. M., & Tummers, L. G. (2015). A systematic review of co-creation and co-production: Embarking on the social innovation journey. *Public Management Review,* 17(9), 1333–57, https://doi.org/10.1080/14719037.2014.930505

Walker, D., Brock, D., & Stuart, T. R. (2006). Faceless-oriented policing: traditional policing theories are not adequate in a cyber world. *The Police Journal,* 79(2), 169–76, https://doi.org/10.1350/pojo.2006.79.2.169

Warren, A. M., Sulaiman, A., & Jaafar, N. I. (2014). Social media effects on fostering online civic engagement and building citizen trust and trust in institutions. *Government Information Quarterly,* 31(2), 291–301, https://doi.org/10.1016/j.giq.2013.11.007

Yardley, E., Lynes, A. G. T., Wilson, D., & Kelly, E. (2016). What's the deal with 'websleuthing'? News media representations of amateur detectives in networked spaces. *Crime, Media, Culture,* 14(1), 81–109, https://doi.org/10.1177/1741659016674045

Žitnik, A., De Vries, A., Reuge, E., Tani, K., Kermitsis, M., Rijken, M., Van Staalduinen, M., Denef, S., & Oggero, S. (2018). Catalogue of Existing Technologies and Solutions. Deliverable 2.2. Medi@4Sec Project deliverable 2.2, http://media4sec.eu/downloads/d2-2.pdf