Police Practice and Research
An International Journal

ISSN: 1561-4263 (Print) 1477-271X (Online) Journal homepage: www.tandfonline.com/journals/gppr20

Managerial approaches to mitigate police professionals' online harms in the United Kingdom

Yen Nee Wong, Shane Horgan & Elizabeth Aston

To cite this article: Yen Nee Wong, Shane Horgan & Elizabeth Aston (26 Jun 2025): Managerial approaches to mitigate police professionals' online harms in the United Kingdom, Police Practice and Research, DOI: 10.1080/15614263.2025.2522835

To link to this article: https://doi.org/10.1080/15614263.2025.2522835

Published online: 26 Jun 2025.

POLICE PRACTICE AND RESEARCH
https://doi.org/10.1080/15614263.2025.2522835

Routledge
Taylor & Francis Group

RESEARCH ARTICLE

OPEN ACCESS Check for updates

Managerial approaches to mitigate police professionals' online harms in the United Kingdom

Yen Nee Wong [a], Shane Horgan [b] and Elizabeth Aston [b]

[a]University of Leeds, School of Sociology and Social Policy, Leeds, UK; [b]Edinburgh Napier University, School of Applied Sciences, Edinburgh, UK

ABSTRACT

In this article, we draw on the concept of misconduct to explore how police organisations frame personnel's online harms and its impact on managerial perceptions and strategies. The aim is to provide insights into whether and how a focus on organisational reputation pervades management practices. Based on 52 semi-structured interviews with police managers from 4 police forces in the United Kingdom (UK) and 46 social media policy documents, guidance and training materials used by 25 UK police services, we explore how police managers interpret organisational messaging in their conceptualisation of responsibilities and operationalisation of strategies to protect police personnel online. Line managers' decisions and actions are largely shaped by, and in turn shape, the organisational culture and ethical climate around online harms. We highlight the need to shift police organisational cultures around online harms towards a duty of care, in part as a timely response to implementing the well-being emphasis in the UK's revised *Code of Ethics* 2024. We present three practical recommendations for organisational leadership and social media policy making in a global context both within and beyond police organisations: (1) national-level advocacy for increased focus on personnel vulnerabilities which supports organisational-level shifts towards, (2) an emphasis on wellbeing, and (3) broader managerial training in online harms management.

ARTICLE HISTORY
Received 25 December 2024
Accepted 11 June 2025

KEYWORDS
Misconduct; online harms; managerial strategies; public-facing professionals; policing; well-being; 3PO

Introduction

Drawing on the concept of misconduct, this article examines police managers' perceptions of, and experiences of managing, police personnel's exposure to online risks and harms within territorial police forces in England and Wales and Scotland, with the aim to derive practical recommendations for a wellbeing-driven management approach. Police services around the globe are increasingly creating a social media presence (Lieberman et al., 2013), with this growing assimilation of digital technologies into police personnel's professional and personal lives increasing their exposure to online harms (Waters, 2012). In her

CONTACT Yen Nee Wong y.wong@leeds.ac.uk University of Leeds, 12.05 Social Sciences Building, 13 Beech Grove Terrace, Woodhouse, Leeds LS2 9DA, UK

commentary, Waters (2012), a Captain in the Police Department in the United States, highlights increased online threats arising from social media relating to online 'cop baiting', increased 'community exposure' of police officers, increased risks of loss of personal information and anonymity on social media platforms facilitating uninhibited, inflammatory targeting of police officers and organisations. It appears that some of the risks Waters (2012) identified are independent of whether police engage on social media in an operational or personal capacity, but more tied to the public-facing nature of their professions. Social media platforms are increasingly weaponised by disgruntled publics to subject police personnel to online violence, privacy violations, and threats which can potentially translate into offline harms. Despite these growing threats police personnel are exposed to through social media platforms, existing literature on police use of social media is centred on operational uses (e.g., Collier et al., 2023; Crump, 2011; Hu & Lovrich, 2019; Procter et al., 2013; Ralph, 2022).

Scholarship on other professions, such as journalists (Chocarro, 2019; Davis Kempton & Connolly-Ahern, 2022; Lewis et al., 2020; Miller & Lewis, 2022; Sampaio-Dias et al., 2023; Waisbord, 2024), academics (O'Meara et al., 2024) and politicians (Erikson et al., 2023; Gorrell et al., 2020; Harmer & Southern, 2023; Ward & McLoughlin, 2020) have however highlighted increased risks of online victimisation due to the public-facing nature of these jobs. Yet, little is known about the digital aggressions and online risks police personnel are exposed to, whether and how these are addressed by the individual and the organisation. Thus far, there are no studies examining the extent to which underlying governance structures in police services influence how police managers address police personnel's online harms. More scholarly work in the policing context is needed to inform the development of practical, empirically informed approaches to mitigate risks and redress online harms experienced by policing professionals.

As a pioneering empirical study, it is key to adopt a non-exhaustive framework to explore online harms in its various forms within the policing context. Thus, we mobilise the Online Harms White Paper's (HM Government, 2020, p. 24) definition of online harms:

> Online content and activity [which] gives rise to a reasonably foreseeable risk of a significant physical or psychological impact on individuals.

This paper makes two key contributions to the policing, socio-legal and science and technology studies scholarship conducted within a global context. First, it moves beyond analyses of social media use in operational policing, to provide insights into the intersectional and cross-contextual influences of professional and personal lives on police personnel's online participation. Second, it expands the police misconduct literature to the virtual realm by investigating its conceptualisation in the context of social media participation and impacts on managerial approaches. The paper addresses two research questions:

(1) How do police organisations frame police personnel's online harms?
(2) What impact does organisational understanding of online harms have on police managers' interpretation of responsibilities and operationalisation of strategies to protect police personnel online?

Social media participation among police and policing organisations

Social media platforms such as Twitter (now X), YouTube, and Facebook are increasingly adopted by law enforcement organisations for public engagement (Hu et al., 2018; Ralph, 2022; Walkington et al., 2019), with both positive and negative impacts. Social media platforms provide a vehicle for enhancing and managing police reputation (O'Connor & Zaidi, 2021; Ralph, 2022; Schneider, 2014; Walby & Gumieny, 2020), monitoring social tensions (Schneider, 2016; Williams et al., 2013), facilitating investigations (Sandberg & Ugelvik, 2016; Yar, 2012), engaging digital citizens in surveillance (Lally, 2017; Nhan et al., 2017; Schneider, 2016), and increasing officer engagement and discretionary effort (Hesketh et al., 2016). However, negative social media content can undermine police legitimacy (Intravia et al., 2020; Mohler et al., 2022). This connection between social media, police reputation and legitimacy led to highly regulated access and use of these platforms among officers (Bullock, 2018). Policing organisations invest significant resources into 'presentational strategies' to promote public support (Bullock, 2016; Schneider, 2016), using social media as 'one of the most powerful tools' for narrative control over how policing is represented to the public (Crump, 2011; Lee & McGovern, 2013, p. 115). Underpinned by a cautious approach, discourse on police personnel's social media participation is largely focused on its potential to cause reputational 'harm' to police services (Foundation, 2014).

Similarly, the scholarship on police personnel's personal social media use beyond the United Kingdom highlights harms to organisational reputation through disreputable online personas, sharing views which impact criminal proceedings and police reputation (Goldsmith, 2015; Kelly, 2014), and undesirable online networks (Goldsmith, 2015). Little is known about the regulation of off-duty social media engagement and its potential harms to officers. Officers' work and private lives are deeply intertwined both in the physical and virtual worlds. Scholars report an erosion of the professional/personal boundaries in police personnel's social media use, such as setting up anonymous 'private' accounts in online forums to participate in alternative spaces for expressing concerns relating to policing issues and extending socialisation, 'cohesion and police solidarity' (Brewer, 2022, p. 1204; Hesketh & Williams, 2017). Working in a highly stressful job conducted within hierarchical organisations, officers' behaviours can often be constrained and governed by strict regulations. Online forums create space for officers to comment on policing issues outside of their professional context, developing support and solidarity through mutual sharing about work-related issues while maintaining anonymity through private accounts. Officers' talks about and social bonding through work within their private, personal space draws attention to the blurring of work/social-life boundary in their online participation. This blurred boundary further complicates what Hesketh and Williams (2017) consider to be a complex regulatory environment with non-uniform applications of social media policies within and across forces. These complexities highlight an urgent need for examining the relationship between regulatory frameworks, organisational culture and managerial strategies around online harms, which this article seeks to achieve.

Misconduct in the digital sphere and the role of organisations

Officer misconduct evades a universal definition in scholarship across the globe, remains actively contested (Kane & White, 2009), and is often used interchangeably with deviance or corruption (Porter, 2021). This terminological vagueness seeps into policies and professional standards in England and Wales (Cawthray et al., 2013; Hough et al., 2018). Similarly, the Baroness Casey Review (Casey, 2023) evades a clear definition of misconduct in its critique of the Metropolitan police service's misconduct structures and processes. Existing studies, mostly on junior front-line officers, describe misconduct to constitute a wide range of behaviours with different degrees of perceived seriousness when on-duty (Hickman et al., 2016), classifiable into criminal offences, 'noble cause misconduct' and corruption (Porter & Warrender, 2009). The newly released *Code of Ethics* (College of Policing, 2024) addressed this vague conceptualisation of misconduct by de-emphasising it, instead presenting ethical principles and expected behaviours as non-statutory, 'aspirational' guidelines, as opposed to predefined standards. Misconduct is more clearly specified in the 2024 *Code of Ethics* as a breach of police regulatory or legislative acts.

Yet, what constitutes misconduct in the digital realm remains vague in both policies and policing literature. Scholars (Cawthray et al., 2013; Kelly, 2014) highlight the use of social media as a form of off-duty misconduct, raising concerns about posts that may conflict with expectations of appropriateness or have potential associations with known criminals. In this paper, misconduct became a concept of relevance and interest to the researchers through the emphasis given to it by most managerial officers in our interviews, despite our invitation to them to discuss online harms more broadly and our not prompting discussions of misconduct. The above focus motivated a retrospective application of the misconduct concept to our analysis, as we reviewed scholarly discussions around misconduct and identified key contributions that our work could make to this scholarship. Specifically, our study draws attention to how online harms can also arise from the publics using digital spaces to magnify or scrutinise officers' behaviours while on-duty, having a negative impact which can extend beyond the workplace into everyday lives. The challenges of drawing a line between online/offline and work/personal highlight the importance of understanding whether and how existing policies and professional standards frame misconduct within the context of the digital realm, and the expectations organisations place on police personnel in relation to their online participation.

Scholars approach police misconduct through a 'rotten apples' or 'rotten barrels' perspective. The former emphasises individual predictors such as race and ethnicity (Kane & White, 2009; Wolfe & Piquero, 2011), gender (Fyfe & Kane, 2006; Greene et al., 2004), rank and experience (Donner & Jennings, 2014; Kane & White, 2009) to be predictors of misconduct. The latter focuses on the institution, attributing misconduct to a 'police/cop culture' (Bowling et al., 2019) which emerges from organisational practices and the nature of the profession (Harris & Worden, 2014; Ingram et al., 2018; Ivkovic & Sauerman, 2013; Ivkovic & Shelley, 2010; Westmarland & Rowe, 2018). Punch (2003, p. 193) expanded on the 'rotten apples/barrels' dichotomy through the concept of 'rotten orchards' constituting a much broader systemic collapse which involves and 'implicate[s] other actors in other segments of the system'.

Key contributions of the study

Existing scholarship globally on social media use among police and police organisations focuses on operational policing, leading to an emphasis on online threats to police legitimacy and organisational reputation, and the centrality of presentational strategies on social media platforms. Such an approach fails to acknowledge the intersectional influences of professional and personal lives on how police personnel use social media and the impacts of online participation on both dimensions of their lives. The misconduct scholarship places key emphasis on the behaviours of police personnel either offline or online, while at the same time providing vague definitions of which behaviours constitute misconduct. Taken together, both lines of literature suggest that online threats and harms emerge largely from police personnel's online behaviours, and that managing misconduct provides an adequate response to risk mitigation. Our study highlights how such a perspective fails to recognise online harms which do not emerge from officers' online activities, but rather from public responses to police officers and policing. This lack of discussion of police personnel's online victimisation implies that police organisations and managers not only lack awareness of such forms of online risks, but are also not provided with evidence-informed risk mitigation strategies to protect police personnel.

In this paper, we advance scholarship on misconduct and social media use by examining how police services frame misconduct within the digital sphere, moving beyond an emphasis on individual behaviours and inappropriateness to examine the complex relationships between officer conduct, organisational strategies, managerial responses, and vulnerabilities to risks and harms in online/offline, on-duty/off-duty contexts. We align with Armacost's (2003, p. 493) positioning of individual officers within the broader organisation and its culture, with supervisors as part of the broader social context within which misconduct happens. Our choice of the 'rotten barrels' approach to online (mis)conduct is informed by our key aim to focus on the organisational level, as opposed to the broader structural factors beyond police organisations.

Methodological approach

This study is part of a broader project on protecting public-facing professionals online (3PO). We adopted a two-part approach to data collection and analysis: (1) a desk review of policies and guidance documents, and (2) semi-structured interviews with police managers. We investigated how police organisations frame online harms through an analysis of 46 documents, constituting social media policies used by 25 police services, broader level reports on media relationships and social media engagement from the Home Office and Independent Office for Police Conduct, protectively marked training materials and intranet resources from partner forces, the College of Policing's (2014, 2024) *Code of Ethics*, and College of Policing's (2013) *Guidance on Relationships with the Media*. Our access to protectively marked documents was facilitated by specific points of contacts (SPOCs), each nominated by the four[1] police forces which committed themselves to be our partners for this UK Research and Innovation (UKRI) funded project and ultimately enabled data collection. Documents were collected through our four partner forces and Google searches using the Boolean operators: 'and', 'or', alongside key search terms: 'social media policy', 'social media guidance', 'online code of conduct',

'misconduct', 'professional standards' and 'UK policing'. Inclusion of non-partner forces in the desk review was dependent on public availability and searchability of documents. This broader representation of UK police forces increases the generalisability of our findings by facilitating an understanding of the organisational framing of online harms on a national and local level. Documents were uploaded onto NVivo for inductive thematic analysis, guided by Braun and Clarke (2006) six-staged approach. Key themes such as professional standards, organisational reputation, personal responsibility, misconduct, complicity and public confidence were identified.

Fieldwork was undertaken across a period of six months, between July and December 2023. We conducted 52 semi-structured interviews with managerial personnel across 4 partner forces who agreed to facilitate access (with at least 8 participants per force), to examine whether and how organisational framing of online risks and harms influences responsibility perception and managerial strategies deployed to minimise risk exposure. The 4 forces are geographically positioned to span the regions of North West England, Yorkshire and Scotland, represent a range of sizes between approximately 3600 to 22,000 police personnel, serve a mix of urban and rural areas with varying degrees of deprivation and affluence, and have both community-based and specialist units handling a broad spectrum of crimes. Geographical and size diversity across these four forces presents a relatively representative picture of police forces across England and Wales and Scotland. Ethical approval was acquired from [Edinburgh Napier University] prior to commencement to ensure that ethical practices of informed consent, non-coercive participation, privacy, confidentiality and duty of care was upheld. Purposive sampling was first used to select interviewees based on their managerial roles and responsibilities within the organisation, and knowledge and experience of managing online harms. We worked with single-point-of-contacts from partner forces for participant recruitment, followed by snowballing where we requested interviewees to connect us with divisions, units or individuals mentioned during the interviews. Participants recruited through snowballing were selected based on interviewees' insider knowledge of their integral management role or specialist understanding of online harms. A participant information sheet was disseminated to potential interviewees, which enabled them to ascertain if they were a good fit and to pose further questions before deciding to participate. 10% of our selected interviewees responded with uncertainties about their abilities to provide useful inputs to the study, with concerns relating to not having encountered online harms in their managerial roles.

We addressed queries from potential participants through email correspondences and initial online meetings, which resulted in a successful recruitment of interviewees representing different (1) levels of understanding of online harms, (2) range of experiences of managing online harms, (3) divisions/units across the service such as professional standards, specialist officers, local and neighbourhood policing, custody, cyber-crime, well-being champions, corporate communications and training and development, and (4) ranks from (detective) sergeants to assistant chief constable for participants who are officers. Three police constables with no managerial responsibilities were included for their expert knowledge on digital platforms and online harms, and lived experiences of online harms as minority officers. All participants had at least 10 years of policing experience. Interviewee diversity enabled us to gain an organisation-wide overview of managerial strategies and perspectives relating to online harms, and to compare practices

across different departmental cultures and composition. Our focus on individuals with managerial responsibilities over public-facing officers meant that managerial officers were more well-represented than staff, at a ratio of 5:1, which we considered appropriate in view of the reporting structures and case management processes adopted by police services.

Semi-structured interviews were conducted and audio-recorded (with consent) on Microsoft Teams, each lasting 60 to 75 minutes. Participants were invited to discuss their experience of managing police personnel's online harms, case handling processes and the resources relied on to facilitate management. Interview questions were framed to identify and understand strategies and best practices used to mitigate online risks, as well as participants' perspectives of where responsibilities should lie in terms of ensuring the online safety of officers. Dikko (2016) highlight that validity in qualitative research is largely dependent on researcher experience and expectations during the interviews. To increase validity, interviews were conducted by highly experienced researchers and interview questions clearly framed, so that data collected directly addresses our research questions. In particular, interviewees were invited to discuss their understanding of online harms to ensure a broad conceptualisation of the term. In the event that only professional or personal social media use were discussed, follow-up questions were used to understand why interviewees only focused on a particular aspect, and prompts were later used to invite them to elaborate on the other. In cases where interviewees presented a narrower focus on misconduct, researchers presented the framing in the Online Harms White Paper (HM Government, 2020) to invite participants to reflect on the psychological aspect and whether and how they recognise it to constitute online harms. Significant efforts were thus made in the clear framing of the questions to obtain a more holistic discussion of online harms which aligns with the definition adopted in this paper.

57 hours of audio recordings were produced and transcribed verbatim by a third-party service provider. Transcriptions were uploaded onto NVivo software for coding after checking and anonymising, with pseudonyms provided by participants themselves. Data analysis was done simultaneously with interviews, such that our decision to stop recruitment was informed by the achievement of data saturation. Given (2016, p. 135) defines saturation as the point at which 'additional data do not lead to any new emergent themes'. After ascertaining that the themes identified through our data analysis were well-developed and that no new themes emerged, we determined saturation was reached. Fereday and Muir-Cochrane (2006)'s approach to thematic analysis was adopted for our analysis, as the hybrid use of deductive and inductive methods facilitate greater articulation of participant voices in relation to themes emerging from our desk review. In deductive analysis, we developed the coding schema based on our research questions and the themes identified in the desk review. We compared our raw interview data against the coding schema and conducted pilot coding. Deductive analysis gave rise to a rigorous framework affirming the relevance of themes in the desk review to the interview data, and revealed other key themes such as risk perception, risk mitigation, harms management and structures of responsibility. Inductive analysis, guided by Braun and Clarke (2006) six stage approach, revealed further subthemes relating to the key themes, such as well-being, care deficiency, manager/officer relationships, (in)visibility of harms, disciplinary measures, resource inadequacy and process-driven investigations. Insights from interviewees were prioritised to highlight police managers' voices on their strategic approaches to addressing police personnel's online harms.

Findings

Themes identified in our inductive and deductive analysis (discussed above) are assimilated to provide responses to the two research questions in this paper. The findings are therefore presented in two parts, the first focusing on the organisational framing of online harms (question 1), and the second on the impact of this framing on managerial perspectives on online harms and strategies to protect police personnel (question 2). In the second part, we highlight how factors such as team composition and departmental culture, as well as the lived experiences of police managers, can influence how they interpret their responsibilities over police personnel's online security and operationalise organisational interpretations of online harms.

Organisational framing of police personnel's online risks and harms

Professional standards, misconduct and well-being

Standards of professional behaviour for members of the policing profession in England and Wales are laid out in the College of Policing (2014, 2024) *Code of Ethics*, which guides the development of policies, guidance, organisational strategies and practices across police services. Underpinned by 'the founding principles of British policing' (Peel's principles), its emphasis is on the maintenance of ethical principles, behaviours and decisions of policing professionals to maintain public trust and legitimacy (College of Policing, 2014, 2024). The 2014 *Code of Ethics* sets out actions to be taken based on the 'type of unprofessional behaviour or misconduct alleged', with 'self-regulation [of] your own behaviour and that of your immediate peers and teams' as the first level of action (College of Policing, 2014, pp. 19–20). Stemming from the national level, this language of 'standards', 'self-regulation', 'misconduct', violations, and management actions attempts to shape the ideologies, decisions and behaviours of policing professionals from their first initiation into the service. The 2024 *Code of Ethics* shifted away from this emphasis on conduct management, instead incorporating a focus on mental, physical and emotional wellbeing and advocates for line management support for wellbeing-related issues. This revision was yet to be introduced at the time of our study, suggesting its impact to be limited.

Organisational reputation, personal responsibility and misconduct

Social media is given brief mention in both the *Codes of Ethics*, stating that 'the standard also relates to the use of any platform of web-based or mobile communications, social networking sites, and all other types of social media' (College of Policing, 2014, p. 11, 2024, p. 10). 'Potential risks' on social media are framed as publishing materials online that 'undermine your own reputation or that of the policing profession or might run the risk of damaging public confidence in the police service', or 'be perceived by the public or your policing colleagues to be discriminatory, abusive, oppressive, harassing, bullying, victimising, offensive or otherwise incompatible with policing principles' (ibid.). Whilst the 2024 *Code of Ethics* included more behavioural recommendations for avoiding online risks, the framing through a professional standards lens remains evident. Online risks constitute misconduct that harms the reputation of the service, with an emphasis on

personal responsibility to ensure online behaviours do not disrepute the organisation or themselves. Such framing is carried through into social media policies, guidance and training materials of police forces across England and Wales. A joint social media policy from Bedfordshire, Cambridgeshire and Hertfordshire Police (2020) specifies that:

> Employees using personal social media account should not post anything which could bring the organisation into disrepute and compromise ongoing operations or investigations.

What constitutes inappropriate posts is clearly specified in policies and guidance. Bedfordshire, Cambridgeshire and Hertfordshire Police's (2020) succinctly states examples of unacceptable online behaviours:

> Posting or sharing of any materials or links to any material that is defamatory against the force, another organisation or individual, [. . .] any material that could be deemed to be offensive, inappropriate or illegal, this includes sharing privately to individuals or groups. [. . .] Police material should not be shared via messaging applications such as WhatsApp'.

Here, social media policies constructed at the local level of police services echo both national level *Code of Ethics* in its emphasis on organisational reputation. However, not all parameters in the policies are clearly specified, with notions of deemed inappropriateness and offensiveness being ill-defined, since these thresholds vary across individuals (Cawthray et al., 2013). Similar to Kane and White (2009) critique of misconduct in the offline context, it remains subjective to contestation within the online sphere with vaguely defined parameters, warranting an examination of whether and how policies and guidance on online harms are translated into practice by police managers.

Organisational divisions in managerial perspectives and strategies

Organisational harms management and structures of responsibility

Within large organisations such as police services, the translation of policies and guidance into effective practice can be complex and challenging. Interviewees highlight unevenness in implementation across different divisions in their organisations. An organisational divide emerges in the management of online participation for work and personal purposes, the former falling within the scope of Corporate Communications (CC) teams, the latter under the responsibilities of Professional Standards (PS) units. Whilst emphasising organisational reputation, both CC and PS teams mobilise different strategies, giving different emphasis to the 2014 *Code of Ethics*. CC teams in all four organisations considered social media engagement for work to be for maintaining public confidence and challenging misinformation about police services. The framing of online messages was key, leading CC teams to develop and deliver detailed guidance, training and feedback to police personnel with official social media accounts, to equip them with skills to mobilise social media for community engagement. Minimising officers' risks of online misconduct is achieved through a template-style shaping of online messaging. A managerial staff in a CC team described this consistency in practice as:

> the corporate style, and it should be that if you are looking at a post, that you or I should never be able to tell that those are written by three or four different people over a period of

> time. On the corporate accounts [. . .], nobody is really identifiable on our accounts [. . .] so I suppose, the risks that we see [. . .] tend to be around content that gets bold [. . .] We have a lot of negative, and quite harmful comments that come our way, when we post about some of our under-represented communities. (na)

The CC teams downplayed harms associated with being targeted by aggressive online comments with the justification that the monitored and centrally managed use of social media platforms and online anonymity of officers sufficiently grants immunity against non-personalised and personalised attacks. Such a risk management strategy deviates significantly from those developed by PS units to regulate social media use on a personal capacity.

Personal responsibility, misconduct and disciplinary measures

The 2014 *Code of Ethics* had most influence over the strategic actions of PS units, centred around preventing misconduct and ensuring personal security online. Police managers in the PS units echo the definition of online misconduct in the 2014 *Code of Ethics*, organisational policies and guidance documents. Examples of inappropriateness are reiterated to police personnel through internal communications materials and training, with the intended outcome of preventing online misconduct through awareness raising. PS units conceive of online personal security within the scope of privacy settings, advising police personnel to ensure the confidentiality of private information (contact details, family members' details, police identity, job role and employer details), and avoid sharing political opinions online. PS units present such advice as recommendations to keep police personnel safe, rather than as expected and required behaviours, due to a recognition by police organisations that the direct regulation of officers' behaviour should only happen on-duty. A police manager from a PS unit added:

> Officers have an absolute right to a private life. [. . .] nobody anywhere is proactively checking police officers' social media input to make sure they are not, you can't do that. That is not fair or right. (Mr White, Inspector)

The need to 'balance officers' right to a private life' (Mr White) with ensuring they abide by the 2014 Code of Ethics meant that messages relating to online risks and personal safety often emphasise online self-regulation to avoid misconduct which threatens career and privacy. Police personnel are advised to stay away from associations with materials which may bring harm to the force, even in their off-duty, personal online engagements. The PS units' dominant message to uphold policing standards, avoid misconduct and ensure personal safety online informed and shaped, to varying extents, police managers' operationalisation of strategies to protect personnel online.

Managerial strategies for online harms vary across divisions and units, with varied emphasis given to managing misconduct, in part attributable to factors such as team composition and departmental culture, personal experience, and interpretation of managerial and personnel responsibilities around online harms.

Team composition and departmental culture

Risk perception and harms management

Managerial strategies can be categorised into two approaches, proactive and reactive, influenced by departmental culture and officers' roles. Line managers working with older, non-frontline officers have less issues with online harms because their team is less active online, informing a reactive approach. Amanda Jane (Sergeant) describes lower levels of online participation in their team:

> I don't want to sound ageist or anything else, but I think maybe younger officers who are a bit more naïve, I might be wrong, they are in bigger divisions with more people. But I think our division, there is not an issue [. . .] you have to apply for specialist roles, so it will be people with, out with their probation, with a bit more experience. [. . .] we don't have that same stressful being on a shift, you know, going to difficult calls, where [. . .] you would be decompressing after it.

Amanda Jane's narrative suggests that online harms emerge differently across the organisation and managerial responses are shaped by different risk landscapes. Like Amanda Jane, most interviewees highlight age, work experience and job roles to be key determinants of departmental culture around online risks. Rebecca (Chief Inspector) neatly sums up the complexity of adopting a one-size-fits-all online harms management approach:

> I guess it would be different across the country, just different experiences, I guess, different demographics of officers and age brackets and service brackets and things, just bring different challenges.

Manager/officer relationships and process-driven investigations

Managers who considered online harms less of a risk to their officers were less likely to echo the organisational emphasis on online misconduct as a preventative measure, tending to act only as middle persons in investigative procedures or signposting officers to sources of help where necessitated. There is a confidence in existing organisational structures providing necessary support to officers without the need for managerial interventions. Coco (Acting Detective Chief Inspector) describes clear processes for seeking help and the secondary role of line managers:

> If an officer received some sort of threat, then the expectation is that they would speak to a supervisor or a trusted person who would then take that forward through the chain of command. Whether it goes to Professional Standards, or whether it is handled in-house, there would be an independent inquiry and supports put in place around that officer and their family. But that's only going to come if the officer discloses it. I would say it's very inclusive and it's very accessible.

Coco's illustration highlights that the availability of services is premised upon the proactiveness of individuals to seek support, placing responsibility on officers to recognise they have been subjected to online harms. Such inclusivity precludes officers without adequate knowledge of online harms or those in divisions which emphasise resilience and frown upon seeking psychological support.

Disciplinary measures and personal responsibility

On the other hand, managers of younger, less experienced officers are unlikely to adopt a reactive approach, perceiving of the treatment of online platforms as digital 'canteen' for officers to destress and gain emotional support (Hesketh & Williams, 2017) as a significant threat. A proactive managerial approach is considered necessary to prevent officers from inappropriately using digital platforms to 'decompress' and relieve stress accumulated through policing work. Bella (Chief Superintendent) describes the risks of bringing 'canteen culture' into the online space, rejecting the act of leaving behind digital footprints of inappropriate behaviour:

> policing is a really intense role [. . .]The thing about the police bar is, you could go into the police bar, you could sit down and you could decompress [. . .] if you've had a really stressful day, you may say something that actually you don't mean because you just need to go, argh [. . .] It's now recorded, social media records things forever, it's there, you can't get rid of it. [. . .] People need to not do it, but that's how people socialise now. [. . .]

In this climate, managers adopt a proactive approach to prevent inappropriate online behaviours, echoing the organisational response to misconduct in policy and guidance materials. Tigger (Inspector) describes how:

> Online presence and the use of WhatsApp groups [. . .] has been something that's been at the forefront of our misconduct investigations for quite a number of years now [. . .] And having worked with student officers predominantly over the last few years, it's just, I think because people are so used to just being able to say or do or have opinion without real consequence.

(In)visibility of harms and care deficiency

There is a perception among line managers that younger, inexperienced officers have different online cultures to themselves and are less attuned to organisational expectations to uphold professional standards of behaviour. Line managers emphasised misconduct to caution officers against sharing inappropriate content online which can damage both the organisations' and their reputations. This focus on officer-generated content implies that other forms of online engagement which may pose risks to officers are given less immediate attention. James (Chief Inspector) reflects on an inadequately managed online harm incident:

> There was someone on my team who was online dating for a significant portion of time [. . .] And I know that she met up with [. . .] men that were undesirable. [. . .] she would joke about the fact that they were very anti-police or when they found out what job she had, the contact soon died down. [. . .] I kind of left her to it and it was a bit of a roll of the eyes. [. . .] Perhaps as a manager I could've done more to take her to one side and discuss her safety and safeguarding and what not.

Even though socialisation on online dating sites can expose officers to targeting due to their police identity, line managers like James can overlook online risks that do not involve misconduct. Managers working with larger teams of younger, inexperienced officers, often framed as likely to transgress in their social media engagement, are more likely to adopt an organisational focus on misconduct, thereby overlooking other forms of potential risks.

However, when online harms translate into physical threats or crimes, line managers more readily recognise and manage these harms, especially where police

personnel have exercised due diligence to minimise exposure to online misconduct. Managers provide guidance and emotional support to officers throughout the resolution or investigation stage, signposting them to support services provided by the organisation. Alice (Inspector) described themselves ensuring a support system was in place for an officer who experienced property damage when their officer identity was revealed online:

> Fortunately, it was a one-off [. . .] if it were to continue then she's got additional security [. . .], cameras to see if we could catch who else was on it. [. . .] there were referrals through to our occupational health unit and line manager really checking in daily and making sure, [. . .] that she was getting supported coming to and from work if she needed to.

Managers' prioritisation of online incidents which culminate in physical harms reveals limited understanding of the nature of online harms, as such a persistent focus on the more familiar landscape of physical threats. Similarly, in contexts where online aggression can be criminalised, police managers are more likely to recognise and act on the harm. A senior officer described an incident of a sexual assault case officer, having their personal details stolen for a fake profile to commit sexual crimes, being efficiently dealt with through investigations and removal of the profile, and wellbeing support for the officer and their family. On the contrary, imagined physical threats yet to be perpetuated or constitute a breach to the legal system (e.g., James' online dating incident), and psychological harms which may not materialise as physical harms, are often not legitimised as online harms. Tigger (Inspector) describes invisibility and silencing around the online victimisation of officers:

> 21 years in the job and I've never heard of anybody in my course that's been tracked down by their social media and harmed as a result of it. [. . .] Because there's more incidents of us doing something wrong in that social media space than someone doing something wrong to us. [. . .] It's not been something that's really played out in the national media either [. . .] When it's not brought to your attention, it's not something that really springs to mind.

Line managers therefore fail to address and mitigate online harms which do not constitute misconduct or physical harms, except for a select few line managers who have experienced and are therefore aware of the complex landscape of online harms.

Lived experience of online harms

Well-being, care deficiency and structures of responsibility

Line managers who have themselves experienced online harms and found it difficult to navigate the organisations' support system recognise the challenges officers face in accessing help. James (Inspector) describes insufficiency in wellbeing support for online harms:

> [T]here could be a lot more investment in support for staff you know, sometimes it does feel a bit tick-box. [. . .] So I think there is an over-reliance on third sector support, and doing support on the cheap, to be honest.

Lived experience, coupled with informal knowledge acquired through risk mitigation efforts, informed a proactive approach to online harms. Managers with lived experience

problematise an organisational approach marked by distinctive divisions in departments, roles and responsibilities across police organisations. Robert (Operational Police Sergeant) highlights the need for integrative, cross-divisional collaborations to tackle online harms:

> Professional Standards probably need to work alongside I think Health and Well-being team. [. . .] so we have a balanced approach to saying, this is what is expected of you online, but if something happens to you, or you are feeling the effects of it, then also, this. But at the moment we just have, don't do this, you know, and nothing about the individual, or overall wellbeing, or isolation.

Robert's narrative demonstrates that collaborative efforts across the organisation is necessary to achieve a holistic online risk management approach which gives even emphasis to both wellbeing and behavioural regulations.

Developing supportive manager/officer relationships

Line managers with lived experience perceive limitations in existing organisational frameworks and are less inclined to adopt the organisational focus on misconduct, tending instead to invest efforts into filling organisational gaps in support provision for officers. A senior managerial staff, Katie, described their experience of online harm informing a proactive push for organisational culture shift:

> When it was happening to me, everybody disappeared and it was only when things had calmed down again that people would come back and [. . .] express their sympathies or show support [. . .] I think through that I worked out who my actual support network was, so I have tried to replicate that in the future [. . .], I got involved in some of the organisational culture work.

Managers like Katie, understand the limitations of self-regulation and organisational support systems as risk mitigation strategies, motivating their wellbeing-focused managerial practices. Katie mobilised their seniority in the organisation to influence organisational strategies by working with the Professional Standards unit to downplay the emphasis on misconduct and raise awareness about different forms of online harms. Others proactively undertake additional responsibilities to look out for officers' online well-being. A line manager described becoming a Wellbeing Champion to provide support to officers they do not directly manage. By taking on the added responsibilities of a Wellbeing Champion, proactive line managers volunteer their time to train as a node of wellbeing support for colleagues in their division, increasing their scope of influence and service within the organisation.

Interpretation of responsibilities for police personnel's online security

Risk perception, misconduct and personal responsibility

Line managers' interpretation of responsibilities over police personnel's online security can influence managerial approaches. Whilst all managers expect police personnel to be responsible for their own online safety, there is little consensus on how and whether responsibilities should be shared with line managers, police organisations and broader governance and legislative structures. Organisational framing of online harms around

officer misconduct shapes managers' understanding of online risks, with most attributing online harms to carelessness, either through inappropriate or unconscientious behaviours. Several interviewees attributed managers' uptake of the organisational messaging around online misconduct to national-level initiatives emerging from incidents with massive media coverage, such as misconduct in the Metropolitan Police. A detective inspector (43qn6) stated:

> Within the Metropolitan Police [. . .] officers that were sharing pictures from crime scenes [. . .] with derogatory comments, [. . .] as a result of that, the reminder of you know, the appropriate use of messaging and private groups and [. . .] a focus on not having those groups where there's not a need to have them.

43qn6 adopts a 'rotten apples' perspective to explain how the 'unacceptable and negative undertakings of a few officers' on social media platforms tainted the reputation of police and policing as a whole, resulting in national-level advocacy for conduct management online. Since media reporting and its associated public discourse play a significant role in shaping policies at the national level, it comes as no surprise that police services and managers became more concerned about officers' (mis)conduct than victimisation when dealing with online harms. Joseph, a detective chief inspector expressed that 'there is a public perception that we should adhere to a particular standard', and that if 'messages that were used on a private social media account fell below that, [. . .] it could impact on public confidence'. An emphasis on content curation so as not to undermine public confidence in the police emerges as a key motivation for managing online risks. Managers also expect officers to regulate their peers' online behaviours, reporting or calling out inappropriate actions. In the words of Bella (Chief Superintendent):

> It is not necessarily what they are putting online but actually if they are in a friendship group [. . .] posting something inappropriate [. . .] they have to call it out, [. . .] just by being present in a group which is espousing values which go against the police service, they are culpable.

Managers place significant responsibility on officers to self-regulate, the failure of which can lead to risks of falling foul of misconduct. Line managers of larger, younger teams of officers, as well as those who attribute responsibility for online security mainly to police personnel, describe consistent reinforcement of this organisational messaging of self-regulation to their teams. Such is conducted through various channels such as verbal reminders during team meetings, sending emails to alert team members to intranet communications about appropriate behaviours and staying safe online, and setting ground rules on work-related WhatsApp groups. Not all managers chose to participate in their teams' WhatsApp groups, with some reporting self-exclusion to avoid the added responsibility of curation, oversight and self-regulation, whilst acknowledging that such a choice may limit their risk mitigation capabilities.

Structures of responsibility over data risk mitigation

Unlike online content creation, most managers consider ensuring online safety through personal data protection to be a shared responsibility between police personnel and police organisations. Police personnel are responsible for ensuring appropriate security settings are in place, while police organisations bear responsibilities for awareness raising

and providing training on online safety. Connor Macleod (Chief Inspector) neatly summarised this as 'a partnership [. . .] understanding that you have a responsibility [. . .] to protect yourself in there. Just that ongoing piece of reassurance and briefing from the organisation as well.'

Some managers suggest that responsibilities over officers' online safety should extend beyond the individual and organisation, to the national level through government initiatives and policies. Sam Vines (Chief Inspector) expresses that:

> We are officers of the crown [. . .] and the Home Secretary's responsibility for policing, absolutely, yeah. I would suggest there's some Government responsibility as well to make sure that the framework is in place for police forces to be able to support the staff. And then by extension the HMIC when they do their inspections of constabulary on behalf of the Home Office, they would hold the force to account for anything that it should be doing to protect its staff.

Beyond a focus on accountability, most find it challenging to articulate what higher-level strategies for ensuring officers' online safety may constitute, pointing to a dominant emphasis on the individual. Line managers' conceptualisation of risk mitigation as individual responsibility meant the emphasis tended to be on behavioural change, either by reinforcing appropriate behaviours or encouraging police personnel to seek wellbeing support.

Discussion

The objective of this paper was to understand, through a managerial lens, whether and how organisational framing of online risks and harms influence police managers' risk mitigation strategies. Our thematic analysis of policy and guidance documents created by police organisations on online social media use reveals an over-emphasis on online (mis) conduct and self-regulation to protect organisational reputation and maintain public confidence in the police. Whilst recent scholarship (Brewer, 2022; Hesketh & Williams, 2017; Kelly, 2014) highlight a blurring of work/personal life boundary in officers' online engagement, our findings suggest that organisational strategies around harms management are unresponsive to this interweaving of police personnel's work and personal identities. Police organisations continue to establish an organisational division in the management of online participation for work and personal purposes. The embedding of personal social media use within the premises of the Professional Standards units informs an emphasis on misconduct, in spite of Cawthray et al. (2013) conclusion on the definitional vagueness of the concept. In response to the lack of clarity in how misconduct is conceptualised by police organisations, existing studies (Hickman et al., 2016; Porter, 2005, 2021; Porter & Warrender, 2009) attempted to categorise different types of offline deviance among police personnel.

Similar studies have not been conducted for online deviance, with the lack in scholarship guiding practice contributing to police services' conflation of online harms with online misconduct and reputational harms. This conflation is in part attributable to reactive responses to a media landscape (see for example Baker, 2024; Dearden, 2021; White, 2024) portraying officers as perpetrators rather than victims of online harms. An undivided focus on protecting organisational reputation suppressed concerns over, and

visibility of, the complex landscape of online harms public-facing police personnel are exposed to both on and off-duty. Limited efforts are thus invested into addressing online vulnerabilities, kickstarting a vicious cycle of invisibility and neglect of online transgressions against police personnel. We conclude that existing guidance and policy on mitigating online risks are limited and lack in responsiveness to the digital landscape. Managerial strategies constructed to echo such organisational framing of online harms can have negative implications for police personnel in terms of limited access to support networks and services.

From our qualitative interviews with managerial police personnel, we found that there was no universal approach to online harms management among police managers, with strategies emerging from an interplay of organisational and departmental culture, nature of job roles, team composition, informal knowledge and lived experiences of managers. Most line managers' understanding of online harms and responsibilities align with the dominant organisational emphasis on upholding policing standards, avoiding misconduct and ensuring personal safety. Our findings are consistent with other studies on the regulation of social media engagement for professional purposes in police organisations (Bullock, 2018; Crump, 2011; Schneider, 2016), where organisational reputation and police legitimacy are primary goals for managing social media use among police personnel. Such emphasis can have negative implications on the wellbeing of police personnel exposed to online harms falling outside managerial notions of what such harms constitute. Our findings draw attention to a diverse landscape of online harms experienced by officers, such as online harassment with the potential to translate into physical harassment, online stalking culminating in damage to physical property, and psychological distress from shouldering responsibilities for online self-regulation.

Existing studies on other public-facing professionals echo similar forms of online harms experienced by police personnel in our study, such as online harassment and abuse which can often be gender-centric (Davis Kempton & Connolly-Ahern, 2022; Harmer & Southern, 2023; Miller & Lewis, 2022; O'Meara et al., 2024; Sampaio-Dias et al., 2023), online threats of physical harm (Miller & Lewis, 2022) and subtle microaggressions which are discriminatory (Harmer & Southern, 2023). Similar to our findings on line managers' treatment of risk mitigation as largely the personal responsibility of officers, the aforementioned scholarship report various coping strategies by individuals such as regulating the number and type of posts and blocking users which can impact career advancement (Davis Kempton & Connolly-Ahern, 2022; O'Meara et al., 2024; Sampaio-Dias et al., 2023), as well as assuming the added burden of emotional labour and development of resilience (Miller & Lewis, 2022; Sampaio-Dias et al., 2023). Such individualised approaches to redressing harms suggest a lack of organisational involvement, a phenomenon described by O'Meara et al. (2024) as 'procedural distancing' which can make online harms unmanageable.

The limitations highlighted in this study, of an individual-centric online harms management strategy framed through the lens of misconduct, reinforce existing scholarship on other public-facing professionals which report challenges associated with the lack of organisational responsibility over employees' online safety. In response to this ubiquity of online harms identified in our study and existing scholarship and lack of organisational care, we present three practical recommendations for organisational change in police organisations, with the potential for translation into other non-policing contexts.

A wellbeing approach to online harms

Shifting towards a wellbeing approach can encourage greater awareness and reporting of a broader range of experienced harms, indirectly combating Ivkovic and Shelley (2010, 2013) 'code of silence' around officers' online behaviours. Scholars examining police well-being in international contexts (Sigad, 2021; Smith et al., 2022) advocate for the importance of emotional and wellbeing support from the organisation, organisational leaders, colleagues and subordinates in enabling officers to develop resilience and minimise 'organisational cynicism'. Police services can do more to draw attention to potential online risks and harms and encourage officers to seek help in the early stages of harms manifestation, facilitating better leverage of support mechanisms provided e.g., through Wellbeing Champions. An organisational focus on police personnel's online wellbeing is needed to drive greater commitment to the psychosocial needs of officers through increased funding, internal service provision or more service providers, and help police organisations to achieve the *Code of Ethics 2024* vision to emphasise police personnel's mental, physical and emotional wellbeing over and above conduct management. This includes ensuring that professional standards investigations can have minimal impact on the well-being of police personnel. This transition will become vital as digitalisation transforms the ways people work and live, and police organisations welcome new generations of datafied personnel. Whilst recommending police organisations to downplay the emphasis on online misconduct, we highlight that the concept remains key towards the management of blatant misconduct such as in the case of the Met Police described above. Police organisations therefore need to achieve a fine balance between discouraging online behaviours which constitute misconduct while ensuring that police personnel's online well-being remains top priority.

Broaden managerial training to include online harms

Providing training to line managers can contribute to more universal and holistic understanding of what online risks and harms constitute. Schafer's (2009) study on police leadership in a global context highlights the significance of developing effective leadership in police services through training, mentoring and experience. Ensuring that line managers are trained and equipped to manage online harms is key towards the effective protection of police personnel online. Our study highlights that line managers receive adequate skills training on the practical aspects of leadership, but an awareness of the online harms landscape and diverse needs of police personnel remains lacking. Lack of familiarity with social media platforms makes it even more challenging for many line managers to advise officers on online data protection and digital footprint minimisation. To ensure that police managers can effectively oversee the online safety of those under their leadership, it is key that adequate resources are invested into training which focuses on understanding the online harms landscape and technicalities needed for addressing harms. An integration of foundational technical skills on cybersecurity and resource materials for signposting officers into training materials is also essential.

National level advocacy for addressing digital harms

Force initiatives are largely shaped by issues on the national landscape. Procter et al. (2013), p. 435) reports a top-down approach in the operational and strategic adoption of social media in UK police services, involving 'a change to existing command structures and a devolution of decision making down the organisation'. To channel more training and support services into addressing online harms, a national-level call for action is necessary. On the national policy and media fronts, more awareness needs to be generated around the emerging risks that police personnel are exposed to in the digital environment, to motivate the injection of resources into developing interventions and support services on the national, local and organisational levels. Advocating for increased attention to the risks and harms associated with digital adoption will spearhead cultural shifts across police organisations away from a focus on misconduct towards a duty of care. A national level call to action would ensure that social media policies and guidance are relevant to recent developments in new media technologies, and in line with the recent *2024 Code of Ethics* shift from misconduct and self-regulation to wellbeing. Greater awareness needs to be created within police organisations of the algorithmic power of online platforms to broaden networking and force connections (Willson, 2017). Such knowledge will enable police personnel to conceptualise a broader subset of risks and harms beyond online misconduct, to acknowledge the work of algorithms in associating their social media accounts with others through algorithmic systems, described by O'Neil (2016) as the 'black box'. Recognising invisible processes on digital platforms will help police managers to understand the challenges and limitations of self-regulation that despite exercising online vigilance, police personnel may still be subjected to online risks due to the public-facing nature of their jobs.

Conclusion

On the policy and practice front, mitigation strategies for police professionals' online harms emphasise misconduct, maintaining police legitimacy and public trust, and upholding organisational reputation. Our findings are reflected in existing scholarship on operational uses of social media (Collier et al., 2023; Ralph, 2022) and officers' online behaviours (Goldsmith, 2015; Kelly, 2014). This paper makes a novel contribution in its mobilisation of the misconduct scholarship to interrogate governance structures shaping managerial personnel's online harms managerial approaches, thus expanding misconduct scholarship into the digital. Our findings highlight that the long-standing *Code of Ethics* governing police practice across England and Wales informs a lens of misconduct which pervades police organisational cultures through officer training, reporting systems and Professional Standards messaging. We conclude that an emphasis on behavioural regulation limits a holistic approach to protecting police personnel from online harms and propose three key recommendations: (1) national-level advocacy for increased focus on officer vulnerabilities which supports organisational level shifts towards, (2) an emphasis on wellbeing, and (3) broader managerial training in online harms management.

Note

1. These were the four partner forces who agreed to provide access and share information with us during the data collection phase of this project's work package.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by the Engineering and Physical Sciences Research Council (EPSRC): [Grant Number EP/W032368/1].

Notes on contributors

Yen Nee Wong is a Lecturer in Sociology and Social Policy at the University of Leeds. Their expertise lies in the ethics of care, (digital) sociology, media and culture, queer theory, genders, sexualities and embodiment. Their current research focuses on online harms and inequalities relating to Artificial Intelligence-driven technologies and social media engagement. They work within multi-disciplinary teams of sociologists, psychologists, criminologists and computer engineers to understand the ethics of AI use from a citizen perspective.

Shane Horgan is a lecturer in Edinburgh Napier University. Shane is currently the program leader for the BSc in Policing and Criminology, and teaches on the topics of; policing and security, cybercrime and cybersecurity, criminological theory, online research methods, criminal justice, and surveillance. Shane is an affiliate of the Scottish Centre for Crime and Justice Research and the Scottish Institute of Policing Research, and also convenes the School of Applied Science Research Integrity Committee. Shane's research interests include the sociological study of cybercrime and cybersecurity, and police responses. In particular, their work has explored how people and organisations make sense of cybercrime and enact cybersecurity behaviours and policies in their routine everyday lives and operations. Shane is in interested in further developing criminological and sociological perspectives on cybersecurity, the policing of cybercrime, and novel ways ICT is deployed in the governance of security.

Liz Aston is a Professor of Criminology at Edinburgh Napier University and has been the Director of the Scottish Institute for Policing Research (SIPR) since 2018. Her expertise centres on local policing and her current research focuses on technology in policing, and the intersect between policing and drugs. Liz was Principal Investigator for the ESRC-funded INTERACT project and a Co-Investigator on the EPSRC-funded 3PO project. She was appointed by the Cabinet Secretary for Justice to establish and Chair the Independent Advisory Group on Emerging Technologies in Policing (2020-2023). Liz is the co-editor of Palgrave's Critical Policing Studies Series and sits on a number of international advisory boards including for the Vulnerability and Policing Futures Research Centre.

ORCID

Yen Nee Wong http://orcid.org/0000-0003-1776-5221
Shane Horgan http://orcid.org/0000-0001-8863-7134
Elizabeth Aston http://orcid.org/0000-0002-9960-6509

References

Armacost, B. E. (2003). Organisational culture and police misconduct. *George Washington Law Review*, *72*, 453–545. https://doi.org/10.2139/ssrn.412620

Baker, M. (2024). Gwent police officers face gross misconduct hearings over WhatsApps. *BBC News*. https://www.bbc.com/news/uk-wales-68619154

Bowling, B., Reiner, R., & Sheptycki, J. (2019). *The politics of the police* (5th ed.). Oxford University Press.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brewer, C. G. (2022). R/ProtectandServe: An exploration of the virtual canteen culture regarding police misconduct. *Policing and Society*, *32*(10), 1193–1208. https://doi.org/10.1080/10439463.2022.2029434

Bullock, K. (2016). (Re)presenting 'order' online: The construction of police presentational strategies on social media. *Policing and Society*, *28*(3), 345–359. https://doi.org/10.1080/10439463.2016.1177529

Bullock, K. (2018). The police use of social media: Transformation or normalisation? *Social Policy & Society*, *17*(2), 245–258. https://doi.org/10.1017/S1474746417000112

Casey, L. (2023). *Baroness casey review. Final report: An independent review in the standards of behaviour and internal culture of the metropolitan police service*. Retrieved January 29, 2024 from https://www.met.police.uk/SysSiteAssets/media/downloads/met/about-us/baroness-casey-review/update-march-2023/baroness-casey-review-march-2023a.pdf

Cawthray, T., Prenzler, T., & Porter, L. E. (2013). Updating international law enforcement ethics: International codes of conduct. *Criminal Justice Ethics*, *32*(3), 187–209. https://doi.org/10.1080/0731129X.2013.860728

Chocarro, S. (2019). *The safety of women journalists: Breaking the cycle of silence and violence: An overview of nine countries. International media support*. Retrieved July 24, 2024 from https://www.mediasupport.org/wp-content/uploads/2019/10/2871-Gendersafety_FINAL_31.10.19_spreads-1.pdf

College of Policing. (2013). *Guidance on relationships with the media*. https://library.college.police.uk/docs/college-of-policing/Media-Relationships-Guidance-2013.pdf

College of Policing. (2014). *Code of ethics: A code of practice for the principles and standards of professional behaviour for the policing profession of England and Wales*. Retrieved July 15, 2023 from https://assets.college.police.uk/s3fs-public/2021-02/code_of_ethics.pdf

College of Policing. (2024). *Guidance for ethical and professional behaviour in policing*. Retrieved January 29, 2024 from https://www.college.police.uk/ethics/code-of-ethics/guidance

Collier, B. (2023). *Influence policing: Strategic communications, digital nudges, and behaviour change marketing in Scottish and UK preventative policing. Scottish Institute for policing research. Future of policing report series*. Retrieved December 14, 2023 from https://www.sipr.ac.uk/wp-content/uploads/2023/08/Ben-Collier-Influence-Policing-Full-Report.pdf

Crump, J. (2011). What are the police doing on Twitter? Social media, the police and the public. *Policy & Internet*, *34*(4), 1–27. https://doi.org/10.2202/1944-2866.1130

Davis Kempton, S., & Connolly-Ahern, C. (2022). "Who's going to be a creep today?" understanding the social media experiences of women broadcast journalists. *Social Media + Society*, *8*(2). https://doi.org/10.1177/20563051221108410

Dearden, L. (2021). *Police watchdog raises concern over 'canteen culture' WhatsApp groups where officers share racist and sexist messages. The Independent*. Retrieved July 20, 2024 from https://www.independent.co.uk/news/uk/home-news/police-whatsapp-groups-sexist-racist-b1952464.html

Dikko, M. (2016). Establishing construct validity and reliability: Pilot testing of a qualitative interview for research in takaful (islamic insurance). *The Qualitative Report*, *21*(3), 521–528. https://doi.org/10.46743/2160-3715/2016.2243

Donner, C. M., & Jennings, W. G. (2014). Low self-control and police deviance: Applying Gottfredson and Hirschi's general theory of officer misconduct. *Police Quarterly*, *17*(3), 203–225. https://doi.org/10.1177/1098611114535217

Erikson, J., Håkansson, S., & Josefsson, C. (2023). Three dimensions of gendered online abuse: Analysing Swedish MPs' experiences of social media. *Perspectives on Politics*, *21*(3), 896–912. https://doi.org/10.1017/S1537592721002048

Fereday, J., & Muir-Cochrane, E. (2006). Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International Journal of Qualitative Methods*, *5*(1), 80–92. https://doi.org/10.1177/160940690600500107

Foundation, P. (2014). *Police use of social media*. Retrieved July 13, 2023 from https://www.police-foundation.org.uk/wp-content/uploads/2017/08/Social_media_briefing_FINAL.pdf

Fyfe, J. J., & Kane, R. (2006). *Bad cops: A study of career-ending misconduct among New York City police officers*. Department of Justice, National Institute of Justice.

Given, L. M. (2016). *100 questions (and answers) about qualitative research*. Sage.

Goldsmith, A. (2015). Disgracebook policing: Social media and the rise of police indiscretion. *Policing and Society*, *25*(3), 249–267. https://doi.org/10.1080/10439463.2013.864653

Gorrell, G., Bakir, M. E., Roberts, I., Greenwood, M. A., & Bontcheva, K. (2020). Which politicians receive abuse? Four factors illuminated in the UK general election 2019. *EPJ Data Science*, *9*(1), 18. https://doi.org/10.1140/epjds/s13688-020-00236-9

Greene, J. R., Piquero, A. R., Hickman, M. J., & Lawton, B. A. (2004). *Police integrity and accountability in Philadelphia: Predicting and assessing police misconduct*. Department of Justice.

Harmer, E., & Southern, R. (2023). Digital microaggressions and everyday othering: *An analysis of tweets sent to women members of Parliament in the UK*. In Schiffrin, A., Koc-Michalska, K., Ferrier, M (Eds.), In *Women in the digital world* (pp. 7–24). Routledge.

Harris, C. J., & Worden, R. E. (2014). The effect of sanctions on police misconduct. *Crime & Delinquency*, *60*(8), 1258–1288. https://doi.org/10.1177/0011128712466933

Hesketh, I., Cooper, C., & Ivy, J. (2016). Well-being and engagement in policing: The key to unlocking discretionary effort. *Policing: A Journal of Policy and Practice*, *11*(1), 62–73. https://doi.org/10.1093/police/paw021

Hesketh, I., & Williams, E. (2017). A new canteen culture: The potential to use social media as evidence in policing. *Policing: A Journal of Policy and Practice*, *11*(3), 346–355. https://doi.org/10.1093/police/pax025

Hickman, M. J., Piquero, A. R., Powell, Z. A., & Greene, J. (2016). Expanding the measurement of police integrity. *Policing: An International Journal of Police Strategies & Management*, *39*(2), 246–267. https://doi.org/10.1108/PIJPSM-09-2015-0104

HM Government. (2020). *Online harms White paper: Full government response to the consultation*. Retrieved February 23, 2024, from https://www.gov.uk/official-documents

Hough, M., May, T., Hales, G., & Belur, J. (2018). Misconduct by police leaders in England and Wales: An exploratory study. *Policing and Society*, *28*(5), 541–552. https://doi.org/10.1080/10439463.2016.1216989

Hu, X., & Lovrich, N. (2019). Social media and the police: A study of organizational characteristics associated with the use of social media. *Policing an International Journal*, *42*(4), 654–670. https://doi.org/10.1108/PIJPSM-09-2018-0139

Hu, X., Rodgers, K., & Lovrich, N. (2018). "We are more than crime fighters": Social media images of police departments. *Police Quarterly*, *21*(4), 544–572. https://doi.org/10.1177/1098611118783991

Ingram, J. R., Terrill, W., & Paoline, I. E. A. (2018). Police culture and officer behaviour: Application of a multilevel framework. *Criminology*, *56*(4), 780–811. https://doi.org/10.1111/1745-9125.12192

Intravia, J., Thompson, A. J., & Pickett, J. T. (2020). Net legitimacy: Internet and social media exposure and attitudes toward the police. *Sociological Spectrum*, *40*(1), 58–80. https://doi.org/10.1080/02732173.2020.1720554

Ivkovic, S. K., & Sauerman, A. (2013). Curtailing the code of silence among the South African police. *Policing: An International Journal of Police Strategies & Management*, *36*(1), 175–198. https://doi.org/10.1108/13639511311302533

Ivkovic, S. K., & Shelley, T. O. (2010). The code of silence and disciplinary fairness: A comparison of Czech police supervisor and line officer views. *Policing: An International Journal of Police Strategies & Management*, *33*(3), 548–574. https://doi.org/10.1108/13639511011066908

Kane, R. J., & White, M. D. (2009). Bad cops: A study of career-ending misconduct among New York City police officers. *Criminology and Public Policy*, *8*(4), 735–767. https://doi.org/10.1111/j.1745-9133.2009.00591.x

Kelly, A. (2014). Managing the risks of public discourse on the New South Wales police force Facebook site. *Salus Journal*, *2*(1), 19–42.

Lally, N. (2017). Crowdsourced surveillance and networked data. *Security Dialogue*, *48*(1), 63–77. https://doi.org/10.1177/0967010616664459

Lee, M., & McGovern, A. (2013). *Policing and media: Public relations, simulations and communications*. Routledge.

Lewis, S., Zamith, R., & Coddington, M. (2020). Online harassment and its implications for the journalist-audience relationship. *Digital Journalism*, *8*(8), 1047–1067. https://doi.org/10.1080/21670811.2020.1811743

Lieberman, J. D., Koetzle, D., & Sakiyama, M. (2013). Police departments' use of facebook patterns and policy issues. *Police Quarterly*, *16*(4), 438–462. https://doi.org/10.1177/1098611113495049

Miller, K., & Lewis, S. (2022). Journalists, harassment, and emotional labour: The case of women in on-air roles at US local television stations. *Journalism*, *23*(1), 79–97. https://doi.org/10.1177/1464884919899016

Mohler, M., Campbell, C., Henderson, K., & Renauer, B. (2022). Policing in an era of sousveillance: A randomised controlled trial examining the influence of video footage on perceptions of legitimacy. *Policing & Society*, *32*(1), 52–70. https://doi.org/10.1080/10439463.2021.1878169

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

O'Connor, C. D., & Zaidi, H. (2021). Communicating with purpose: Image work, social media, and policing. *The Police Journal*, *94*(3), 333–352. https://doi.org/10.1177/0032258X20932957

O'Meara, V., Hodson, J., Gosse, C., & Veletsianos, G. (2024). Invisible, unmanageable, and inevitable: Online abuse as inequality in the academic workplace. *Journal of Diversity in Higher Education*. https://doi.org/10.1037/dhe0000545

O'Neil, C. (2016). *Weapons of math destruction. How big data increases inequality and threatens democracy*. Broadway Books.

Porter, L. E. (2005). Policing the police service. Psychological contributions to the study and prevention of police corruption. In L. J. Alison (Ed.), *The forensic psychologist's casebook: Psychological profiling and criminal investigation*. (pp. 143–169). Willan.

Porter, L. E. (2021). Police misconduct. In R. G. Dunham, G. P. Alpert, & K. D. McLean (Eds.), *Critical issues in policing: Contemporary readings* (pp. 261–278). Waveland Press.

Porter, L. E., & Warrender, C. (2009). A multivariate model of police deviance examining the nature of corruption, crime and misconduct. *Policing and Society*, *19*(1), 70–99. https://doi.org/10.1080/10439460802457719

Procter, R., Crump, J., Karstedt, S., Voss, A., & Cantijoch, M. (2013). Reading the riots: What were the police doing on Twitter? *Policing and Society*, *23*(4), 413–436. https://doi.org/10.1080/10439463.2013.780223

Punch, M. (2003). Rotten orchards: "pestilence", police, misconduct and system failure*. *Policing and Society*, *13*(2), 171–196. https://doi.org/10.1080/10439460308026

Ralph, L. (2022). The dynamic nature of police legitimacy on social media. *Policing and Society*, *32*(7), 817–831. https://doi.org/10.1080/10439463.2021.1956493

Sampaio-Dias, S., Silveirinha, M., Garcez, B., Subtil, F., Miranda, J., & Cerqueira, C. (2023). "Journalists are prepared for critical situations … but we are not prepared for this": Empirical and structural dimensions of gendered online harassment. *Journalism Practice*, *18*(2), 301–318. https://doi.org/10.1080/17512786.2023.2250755

Sandberg, S., & Ugelvik, T. (2016). Why do offenders tape their crimes? Crime and punishment in the age of the selfie. *British Journal of Criminology*, *57*(5), 1023–1040. https://doi.org/10.1093/bjc/azw056

Schafer, J. A. (2009). Developing effective leadership in policing: Perils, pitfalls, and paths forward. *Policing: An International Journal of Police Strategies & Management*, *32*(2), 238–260. https://doi.org/10.1108/13639510910958163

Schneider, C. J. (2014). Police presentational strategies on Twitter in Canada. *Policing and Society*, *26*(2), 129–147. https://doi.org/10.1080/10439463.2014.922085

Schneider, C. J. (2016). *Policing and social media* (1st ed.). Lexington Books.

Sigad, L. I. (2021). "It gave me the strength and will to continue and to overcome": Police officers constructing resilience while under threat from criminals. *Policing an International Journal*, *44*(1), 93–105. https://doi.org/10.1108/PIJPSM-01-2020-0004

Smith, C. J., Han, Y., Dupré, K. E., & Sears, G. K. (2022). Perceived organizational support and its interaction with voice on police officers' organizational cynicism, stress and emotional exhaustion. *Policing an International Journal*, *45*(2), 200–217. https://doi.org/10.1108/PIJPSM-07-2021-0093

Waisbord, S. (2024). Mob censorship: Online harassment of US journalists in times of digital hate and populism. In O. Westlund, R. Krøvel, & K. Skare (Eds.), *Journalism and safety* (pp. 30–46). Willan Publishing.

Walby, K., & Gumieny, C. (2020). Public police's philanthropy and Twitter communications in Canada. *Policing an International Journal*, *43*(5), 755–768. https://doi.org/10.1108/PIJPSM-03-2020-0041

Walkington, Z., Pike, G., Starthie, A., Havard, C., Harrison, V., & Ness, H. (2019). Entitlement to tell on police Facebook sites. *Cyberpsychology, Behaviour, and Social Networking*, *22*(5), 355–357. https://doi.org/10.1089/cyber.2018.0502

Ward, S., & McLoughlin, L. (2020). Turds, traitors and tossers: The abuse of UK MPs via Twitter. *The Journal of Legislative Studies*, *26*(1), 47–73. https://doi.org/10.1080/13572334.2020.1730502

Waters, G. (2012). *Social media and law enforcement. Potential risks. FBI law enforcement bulletin*. Retrieved April 10, 2025, from https://leb.fbi.gov/articles/featured-articles/social-media-and-law-enforcement

Westmarland, L., & Rowe, M. (2018). Police ethics and integrity: Can a new code overturn the blue code? *Policing and Society*, *28*(7), 854–870. https://doi.org/10.1080/10439463.2016.1262365

White, N. (2024). *Met police under fire for 'racist' emoji on social media photo. The Independent*. Retrieved July 20, 2024 from https://www.independent.co.uk/news/uk/home-news/emoji-emojigate-met-police-racism-b2580422.html

Williams, M. L., Edwards, A., Housley, W., Burnap, P., Rana, O., Avis, N., Morgan, J., & Sloan, L. (2013). Policing cyber-neighbourhoods: Tension monitoring and social media networks. *Policing and Society*, *23*(4), 461–481. https://doi.org/10.1080/10439463.2013.780225

Willson, M. (2017). Algorithms (and the) everyday. *Information, Communication and Society*, *20*(1), 137–150. https://doi.org/10.1080/1369118X.2016.1200645

Wolfe, S. E., & Piquero, A. R. (2011). Organizational justice and police misconduct. *Criminal Justice & Behavior*, *38*(4), 332–353. https://doi.org/10.1177/0093854810397739

Yar, M. (2012). Crime, media and the will-to-representation: Reconsidering relationships in the new media age. *Crime, Media, Culture*, *8*(3), 245–260. https://doi.org/10.1177/1741659012443227