3PO Briefing Series

Issue 3
January, 2024

Specialist Officers

Dr Kris Christmann
University College London

Dr Ingolf Becker
University College London

Grant Ref: EP/W032368/1

UKRI Engineering and Physical Sciences Research Council

The Problem

We live in an age where information and communication technology make it possible to gather, process and analyse information about public officials that had previously been considered private. Social media apps, self-tracking devices, smartphones, CCTV, web-based services, and search engines register personal information about individuals on a scale and in ways that most do not notice or imagine. As more and more of this personal information is collected, collated, stored and analysed by private and public organisations and individuals, so too increases the dangers and risks to public officials. For instance, police officers are increasingly subject to being filmed and that material being uploaded to a mass audience, which represents a 'new visibility' open to use for malevolent or criminal purposes (i.e. 'digital vigilantism', 'trial by social media', online harassment, or just unwanted identification, to name a few). Visibility can here have a *strategic* purpose, in which data trails can be mobilised as an OSNIT tool for information probing to target, intimidate, harass and undermine those working in the public eye. The unwanted revealing ('leakage') of such information can have dramatic repercussions for officers' private lives and that of their families.

The Current Study

Police officers undertake a range of duties and roles. This study examined the specific online risks, harms and privacy needs of 'specialist officers', i.e., those working in high-risk and contentious areas such as counter-terrorism policing, covert/intelligence gathering, cyber-crime investigations, serious and organised crime investigations and a range of specialist public order policing areas. The aim was to capture the impacts of having particular privileged knowledge (i.e., knowing about lawful intrusive data practices) and other role specific risks (e.g., undercover intelligence gathering) that may affect their own privacy perceptions and needs. The working hypothesis is that the online risks and protection needs of specialist officers may differ from the more routine front-line facing police roles (such as neighbourhood policing or patrol policing), and we aimed to explore what these were.

Key Findings

Experiences of online harms

We found that just under half of the specialist officers interviewed (11 out of 24) had experienced a negative online incident as a result of their job (several reported more than one incident). This happened despite them taking some degree of personal security measures to 'lock down' their social media accounts, as well as restricting their online activities and comments/posts. Most reported incidents involved some form of digital vigilantism, often by a single person, which tended to be retaliatory and precipitated by the subject(s) undertaking some form of online open-source research on the officer. A smaller number of instances involved targeting by criminal groups (criminal gangs, terrorist involved groups) and sports 'fanzines'.

The extent to which officers were affected by these incidents varied. Most indicated some temporary effects on their well-being often with a mild effect (i.e., causing some worry and anxieties), whilst several other incidents were more impactful. For some, the online harm temporarily impacted their ability to do their job (in undercover roles but also those working for Police Associations which were targeted by a disgruntled public), although most participants said they carried on without disruption. Most officers we spoke to also managed to avoid negative impacts on their family by not sharing what had happened online (not 'taking the job home'), although this not always possible. There was an acceptance that these types of online incidents were 'part of the job', similar to physical assaults happening to some front-line officers.

Officers' experiences of online risk and threats by specialist roles

Our research shows that online harms and risks can take two basic forms: they can be external threats coming from outside the policing organisation (i.e., the public attacking an officer's individual integrity/credibility) or internal threats deriving from within the organisation (i.e., concerns about transgressing Professional Standards guidelines).

Those working in public order roles reported being most susceptible to unwanted identification and doxing, usually from a recorded 'trigger events' quickly going viral, not helped by how online financial incentives ('clickbait') operate. 'Cop baiting' is a good example, where a posted incident can be staged and/or exaggerated – all of which puts an officer's personal and professional well-being at stake.

Those in undercover/intelligence gathering roles were most likely to avoid all social media activities due to the exposure risks for themselves, operational colleagues and informants. At the same time, these officers reported the highest level of technical support to stay safe online, one that could be considered as a 'gold standard'. This reflects the threat environment they work in, but was seen by several as being more about addressing operational needs than concern for officer's/dependent's safety.

The advocacy nature of some Police Associations (incl. EDI goals such as LGBTQ+) can increase officer's exposure to assorted online harms. Instances of public online abuse occurs towards some prominent Association staff, as well as being aimed at the wider Association mission itself. Such Police Associations have 'blurred lines' as they sit within and without force structures, complicating organisational responses.

Those working in cybercrime/cyber-security and intelligence gathering roles felt most able to protect themselves online. This was due to a combination of technical know-how, 'trade-craft' skills and heightened security awareness (both from formal training and informal learning). Hence, those in the least public facing roles showed the highest threat awareness and ability to stay safe online, whereas more front-line roles reported far lower levels of training and support to tackle online harms. What there is tends to be limited to generic force-wide online 'security messaging' but little, if any, technical ('how to') information relayed at force-level.

Perceptions of Support Available for Officers

A range of views were expressed about the type and adequacy of support available by their employers to keep them safe online. A majority thought there was suitable support in place for officers experiencing online threats and risks, although some others strongly disagreed. There was also a more mixed response from those that had actually experienced an online harm: some reported good experiences after an incident, whilst others did not. For the majority who had *not* experienced online harms, confidence was often expressed in the abilities of their line manager to provide guidance, advice and where needed, to escalate matters for appropriate referral and assistance. The importance of line managers likely reflects the fact that many specialist officers benefited from working within close-knit teams, some of which could access a range of high-level technical skills to investigate and address online threats. Those involved in specialist public order duties reported higher levels of online targeting and less technical support.

Confidence was greatest where an online incident crossed a criminal threshold (constituting an offence), whilst some participants felt that incidents below this threshold restricted what could reasonably be done. In part, this appears to be due to the online threat not easily fitting within provisions designed for an analogue age and to the reactive nature of such provisions. The question of 'legality' framed a lot of discussion about expectations of support, as did notions of personal responsibility for online safety and not leaving oneself open to being targeted.

Support for Officer's partners and children

Most respondents thought that support available for their partners and children was likely going to be inadequate, and that more needed to be done. Responsibility for supporting partners and children tended (although not always) to be seen as the responsibility of the employing police force. As with officers, there was more confidence in official responses if an online harm crossed the criminal threshold than for incidents sitting below that threshold.

Those working in cyber security generally wanted a more robust and inclusive approach to supporting family members and were most critical of the failings of the current limited, if any, provision available.

Early Draft Recommendations

1. Some specialist policing roles are particularly vulnerable to online risks (notably unwanted identification and doxing) and as such should benefit from enhanced protective measures, guidance and support.
2. More needs to be done to raise awareness amongst police officers about online risks and protective measures, including some working in specialist roles. Positive strategies should be used to change behaviour over the longer term (to avoid the problem of short-term shifts) supported by anchoring 3PO advanced tools for online safety. As this is a national issue, responsibility for implementation lends itself to a lead agency with national reach.
3. Police line managers play a pivotal role as 'first responders' to officers reporting online harms and concerns. As such police forces need to ensure that these officers are trained and equipped to guide, advise and (where necessary) refer cases that are brought to their attention and ensure officers are adequately supported.
4. More needs to be done to protect police officers' partners and families from online risks and harms which derive from having a family member as a police officer. This is generally the case for specialist officers, as well as those in more front-line roles. Provision could take a number of forms but needs to firmly address the threats posed by an adversary's 'trade-craft' in identifying family members in order to target police officers. Options could include developing a 'family version' of any tools or guidance provided to police themselves. A further consideration is how 'family online safety' is achieved. This is not merely a technical matter but also one of negotiated settlement to achieve compliance when faced with conflicting interests (e.g., protection needs of the officer parent vs teenage children's desire for wide online social networks). Therefore, thought should be given in providing guidance for officers how to best approach these conversations to reach optimal bargaining outcomes for all concerned.

CENTRIC
Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research

Centre for Criminology, University of Oxford

Edinburgh Napier University
SiPR Scottish Institute for Policing Research

University of Cambridge Institute of Criminology

Sheffield Hallam University
Knowledge Applied
Centre for Behavioural Science and Applied Psychology

UCL Security & Crime Science

Police Scotland
Police Service Northern Ireland

@3po_project
3po@shu.ac.uk
@3po_project
3po-project.co.uk