



Year 2 Report



Contents

Foreword	4
Review and Outlook	5
Online risks and protection needs of frontline officers and staff	6
3PO in South Yorkshire Police	8
Nationals survey: Selection of preliminary findings.....	9
Online experiences and attitudes of children of police officers	11
Social media analysis	13
Managerial perspectives	15
Police Scotland wellbeing event	17
Ongoing research: privacy walks to understand online behaviours and online risk prevention	18
Ongoing development: Self-assessment tool to review online exposure on private accounts	19
Festival of Privacy - REPHRAIN.....	20
3PO symposium - October 2023	22
World cafés - May 2024.....	25
Publications	27
Presentations	28
Information	28

Foreword



Professor Saskia Bayerl
3PO Principal
Investigator, CENTRIC

The second year of 3PO has built on the successes of the previous 12 months, and I am extremely proud of the work done by our academic, police, and Home Office partners. I would also like to express my gratitude to everyone involved in the empirical work in the second year.

The research that underpins 3PO has continued to develop and mature to the point where we can start formulating evidence-based recommendations and test practical approaches with our partner forces. This report is a snapshot of our activities in year 2 and a short digest of results.

I hope you find the second 3PO Summary Report insightful and impactful, and I look forward to the work and findings in the project's final year.



Review and Outlook



Chris Spencer
3PO Project Manager,
CENTRIC

Year Two Overview

The 3PO project has continued to develop and mature over the past year and has been working closely with police partners to bring to fruition training materials, software tools and guidance to support the protection of police officers, staff and their families. We also continue to accrue knowledge about the extent of online harms and their impacts.

Throughout the year, our academic and police partners have met to discuss results and their impacts, including at 3PO consortiums and during the first multi-stakeholder symposium in Edinburgh. Each project event has sparked thoughtful discussions and provided valuable feedback on the project and its direction.

We also managed to increase public awareness by engaging in public discourse on online harms and public-facing professionals and their dependants. Additionally, project members have championed 3PO at various academic and practitioner-focused events.

This 2-year report provides an overview of core insights gathered and events.

Year Three: Looking Forward

As 3PO moves into the final year, the project will consolidate the knowledge collected by seeking to operationalise the research into purposeful solutions. This will include, a fully developed self-assessment tool to be used by members of the police and their dependants; finalising and completing the delivery and testing of training that supports improved officer, staff and dependants skills, attitudes and behaviours towards prevention, identification and mitigation of online risks and harms; and the delivery of policy recommendations to senior leaders and stakeholders that will address key themes which have been identified during 3PO's tenure. The project will also seek to produce operational material that can be used to help support navigating online harms within public-facing professions.

Finally, we look forward to a number of events planned over the next months to turn our findings into concrete, practical approaches, in the form of world-cafes, policy roundtables and the final 3PO Symposium in March 2025.

Online risks and protection needs of frontline officers and staff



Dr Kate Whitfield

CeBSAP, Co-Investigator, Sheffield Hallam University

Frontline officers and staff face specific challenges with different forms of visibility as part of their work. This is compounded by the merging of online and offline life experiences, and can impact police professionals and their families in their personal lives outside of work. This impact has never been fully explored. Consequently, this research aimed to understand the online risks frontline officers and staff face in their personal life as a result of their professional role.

Interviews were conducted with 61 frontline officers/staff and 12 partners of frontline officers/staff. This was a diverse group in terms of years in force, experience in role, and age. All use the internet for personal activity in some way, and most have social media profiles. The interviews were analysed using thematic analysis, which identified four themes:

1. Vulnerabilities, Risks and Threats: This theme highlights how negative lived experiences present themselves. External threats relate to bad actors aiming to harm or gain leverage over police officers/staff directly or through their families. This can occur in many ways, but was most regularly identified in the form of hacking, creating false reports about an officer, cyber-harassment, direct threats, unwanted identification, and malicious accusations. Internal risks were concerns about social media and online information being used within force for disciplinary action or impacting future career prospects. It is important to note that the focus was not on online use that was obviously a matter for disciplinary action, but rather lack of awareness or 'grey areas', where it was unclear of appropriateness.

2. Digital Discretion and Boundary Management:

This theme relates to how police officers/staff protect themselves and their families online by being discreet and carefully managing boundaries. Many obscure their online identity in some way, make themselves unsearchable, and keep settings locked down to only family and close friends. Boundary setting and the compartmentalisation of professional and personal life takes place to prevent potential risks from work overflowing into personal online life. This can mean adopting a more passive role on social media and being an 'observer' of online life.

3. Reporting Incidents and Psychological Harm:

Knowledge and awareness of reporting online incidents varied across the forces taking part in the study. While some officers/staff showed a clear understanding of how to report incidents and knew what the response would look like, this was not always the case. Triggers for reporting issues were often unclear, with officers/staff framing significant trolling and online abuse as acceptable and 'part of the job'. The psychological harm of these experiences was not always viewed as serious as physical harm, and in some forces, the response heavily depended on line managers' knowledge and experience.



4. The Changing Nature of being a Police Officer/Staff:

The context of policing has shifted significantly since the prolific use of the internet in daily life. There is a certain amount of normalisation regarding trolling, with common acceptance that the public-facing nature of policing means officers/staff 'get more stick'. Threats experienced online are quickly dismissed, as they are 'only' online. However, as online and offline spaces are becoming increasingly interconnected, there is acknowledgement that these online threats should be viewed as seriously as physical threats.

As public-facing professionals, police officers/staff need to be especially careful when using the internet, as risks from their work life can spill over into their personal life. Safety measures can be used to protect police officers, staff and their families, alongside employing

digital discretion and strict boundary management between professional and personal lives. However, this requires constant vigilance and can be highly stressful. In some forces, clarity is needed regarding how and when negative online incidents should be reported, as well as guidance in relation to support to ensure a more consistent approach. Further work is also required to encourage greater parity between responses to physical and psychological harm, and recognition of the impact negative online experiences can have on individuals' mental health. The broader context of policing has changed, with online life now as 'real' as in-person life. This carries additional risks, threats, and harms, which need to be considered in terms of their impact on officer/staff well-being.

3PO in South Yorkshire Police



Inspector John Crapper
South Yorkshire Police

South Yorkshire Police has been delighted to be part of the research into this under-explored area.

The UK police forces did not appreciate the extent to which officers' and staff's lives and wellbeing can be affected by online harm. The harm can take many forms and at its worst, can lead to officers being physically targeted or having their safety put at risk.

Even when things do not reach the point of physical harm, unwarranted contact by strangers or critical comments aimed at officers in social media can have an impact which the police service has not been ready to respond to. It also won't be a surprise to readers to hear that female officers are disproportionately targeted by people in the online world. Just as female politicians and television stars receive unbearable abuse, so it is with the police.

Not only is the work of 3PO good for the wellbeing of the police workforce, it is good business sense for the forces as well. A happy workforce will perform better, which has to be good for the force. Some of the potential harm from online threats can include attempts to blackmail officers or cause them to inadvertently disclose private information, which poses clear risks to the police forces as well.

The research will help forces and its workforce with how to reduce the risk that online harm can pose. The police workforce can comprise of some members who

have a high level of technical expertise through to some with almost none. Officers at both ends of the spectrum can be at risk though, as whilst those who have good technical skills may believe they are using online facilities safely, they may not appreciate the risks that they can be exposed to. Officers who have far fewer skills may try to protect themselves by having to withdraw altogether from online activity, which cuts off many aspects of modern life from them. They may then outsource their online activity to a family member, which places needless burdens on others and means that someone with less appreciation of the potential policing risks is carrying out online activity instead.

Police forces have until now largely seen the online world as a risk to reputation of the organisation. I hope that they will adopt the research which 3PO will publish and understand that whilst a reputational risk exists, the forces have an opportunity to positively contribute to the safety of their workforce and to provide supportive advice which will help to protect members of the force, as well as the forces themselves.

Nationals survey: Selection of preliminary findings

Dr Charlotte Coleman
CeBSAP

The national survey aims to provide a view on the prevalence of online harms across police officers and staff in the UK police forces. It was conducted as an online survey, open to all police personnel in the UK.

Here we report preliminary results from a first trench of 758 responses across 14 police forces. Of those responding, the mean age is 39.5 years, 74.5% are male, and all but 14% of the respondents identify as White British.

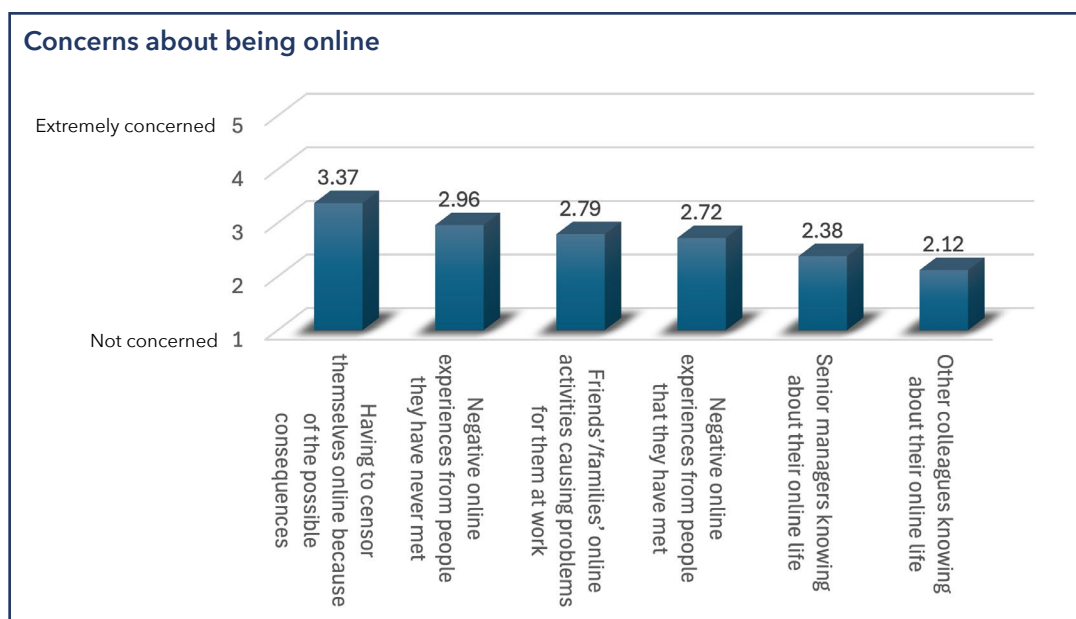
Selected findings

Risk perceptions and concerns

Respondents generally felt they were at risk of negative online experiences **both in their work life** (mean = 3.08 with 5=Very high risk; 3=Moderate risk; 1= No risk) and **in their personal life** (mean = 3.29). They also perceived **their families** to be at least moderate risk from online harms (mean = 2.93).

Respondents were most concerned about their **friends'/ families' online activities causing problems** for them

at work (mean = 2.79 with 5=Extremely concerned; 1=Not at all concerned) and even more concerned about **having to censor themselves online** because of the possible consequences (mean = 3.37). Further concerns were about the risk of negative online experiences **from people that they have met** (mean = 2.72) than those **they have never met** (mean = 2.96). They were further somewhat concerned about **senior managers knowing about their online life** (mean = 2.38), less so about **other colleagues knowing about their online life** (mean = 2.12).



Type of experiences

For many respondents (21.9%) the negative online experiences they had **only happened online**, for others **they started offline and moved online** (15.2%), while for a very small group **they started online and moved offline** (1.7%). Families of police officers had few negative online experiences but were still experiencing some incidents due to their family member being in the police (mean = 1.70 with 5=Very often; 1= Never).

While the frequency of negative online experiences was not high (mean = 1.99 with 5=Very often; 1=Never), they **did impact negatively upon wellbeing** (mean = 2.72; 5=Extremely negative impact; 1=No impact).

Acceptance of online risks and harms

Participant largely found that **negative online experiences are not 'part of the job'** (mean = 2.61 with 5=Strongly agree; 1= Strongly disagree), and even less that it is acceptable that such experience should be considered part of the job (mean = 1.79). At the same time, they felt it **somewhat acceptable to restrict their personal online presence** because they work for the police (mean = 3.41; 5=Completely acceptable; 1= Not at all acceptable).

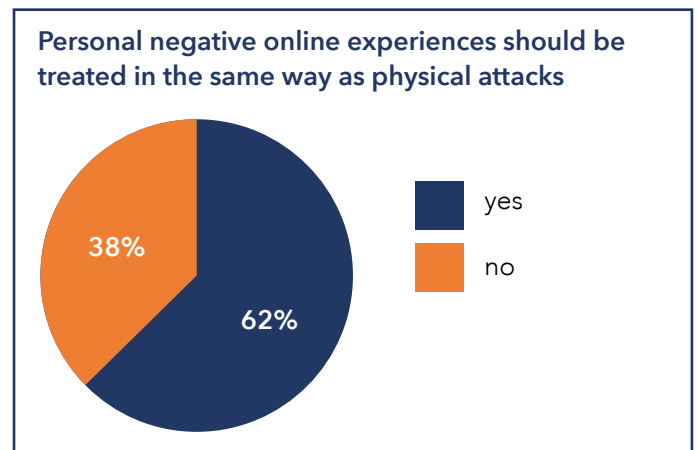
Experiences of support

Respondents who had experienced incidents felt **somewhat supported by their police force** (mean = 2.61 with 5=Completely supported; 1=Not at all supported). However, a considerable number of respondents (116) **did not report** the incident(s). Respondents did draw upon both **formal and informal sources to help protect themselves** online, the most often using trial and error

by myself followed by guidance provided by the police force. However, all sources were used only rarely to occasionally.

Most respondents felt it **appropriate that their force should provide guidance on their personal online presence** (mean = 4.14 with 5=Definitely appropriate; 1=Definitely inappropriate) but felt that the **guidance could be improved** (mean = 2.47 with 4=Excellent, 1= Needs improvement) as could be the **amount of support** available (mean = 2.11 with 5=A great deal available; 1=None).

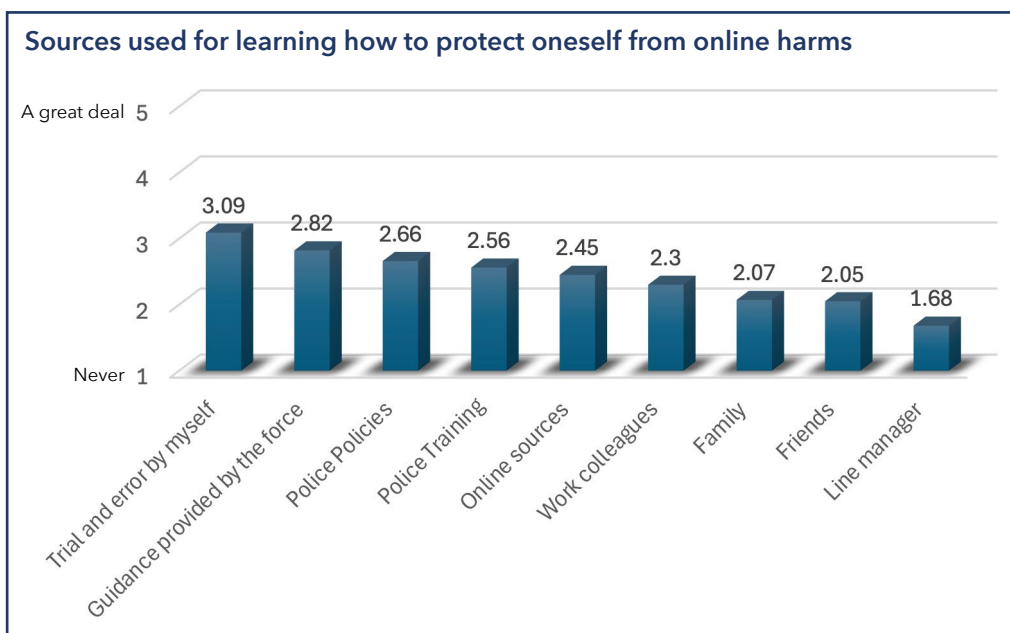
Further, most participants felt that personal negative online experiences **should be treated in the same way as physical attacks** (yes 62%, no 38%).



Note on the data and next steps

The findings are a selection of the full survey and based on a preliminary analysis with the sample available in August 2024. Therefore, results may change somewhat

once the full sample is available. Analyses of the full data are ongoing and will be reported in subsequent publications.



Online experiences and attitudes of children of police officers



Dr Lasara Kariyawasam
Postdoctoral Research
Fellow, University of Oxford



Dr Katrin Mueller-Johnson
Associate Professor of
Criminology and Research
Fellow, University of Oxford

The 3PO team at Oxford University focused on exploring the social media use and attitudes towards online safety among teenage children of police officers. Thirty-one individual interviews and one focus group with five teenagers were conducted. All participating children had at least one police officer parent, were aged 13-17 years, and were active on the internet.

This study aimed to achieve the following:

1. What is it like for children of police officers growing up?
2. How do children of police officers use social media whilst navigating restrictions and demands of parents?
3. What online safety measures do children of police officers take, and what are the possible risky behaviours they engage in online?

Key findings

The findings revealed that most children of police officers have been subjected to ridiculing or bullying by peers at school due to their parents' policing profession. Children were also aware of the negative public's perception of police and the dangers of being a police officer. Almost all participants had seen or come across negative social media content about police officers (e.g., memes or posts ridiculing police officers, videotapes of police officers on duty and hundreds of comments criticising the police).

Whilst the children were aware of the risks of their parents' policing profession, they were still active on several social media sites with Snapchat and TikTok being the most popular platforms. All children discussed having had conversations with their parents around social media safety and some children mentioned having had arguments and disagreements over what they could and could not do online. However, most conversations with parents seemed to have happened only when the children received their first mobile phone and/or when children first started to use social media.

Most children claimed to stay safe online with many of them having private accounts, only adding people they knew in person, and not oversharing online. Whilst this was discussed by many, it seemed that children were most careful and least active on platforms that their parents were using (e.g., Facebook, Instagram), and less careful and more active on platforms that their parents had little knowledge about (e.g., BeReal, Snapchat,

Gaming Apps). Several children discussed being on gaming and messaging applications such as Discord, where they messaged and called unknown people.

Recommendations

Based on the early findings, we recommend the following:

- Police officers with children should be aware of the potential that their children may be targeted with negative messages online due to their parents' profession. This may not be confined to social media but can also extend to gaming platforms.
- In addition to the standard talks about online safety, parents should have early and frequent conversations with their children about social media and the potential harms they might encounter, including how to keep themselves safe online [include practical settings, avoidance of photos etc].
- Officers with children should think consciously at which age their children are given access to smartphones/social media on other devices.
- Schools and other sources (e.g., police forces and tech developers) that conduct awareness and educational workshops on social media safety should consider using more interactive 'game-like' technical tools to engage young people into making sensible decisions when online.

Key activities

Early findings were presented at the following events:

- REPHRAIN all hands meeting in London (September 2023)

- 3PO Consortium in London (March 2023)
- 3PO Consortium in Edinburgh (October 2023)
- University of Oxford Criminology centre's informal seminar (February 2023)
- Family liaison officer conference in Edinburgh (March 2024)
- 3PO Consortium in Oxford (March 2024)
- Thames Valley Police conference (April 2024)
- 3PO world café in Belfast (May 2024)
- REPHRAIN lunchtime talks (June 2024)
- Cyberpsychology conference (July 2024)
- EAPL conference in Portugal (July 2024)
- The American Society of Criminology Annual meeting in San Francisco (November 2024)

Next steps

The team members at Oxford University are also currently conducting a privacy walks study among teenage children of police officers. The aim of this study is to conduct a practical interactive session to understand how children set up social media profiles and maintain these. Next steps include:

- Completing the 'privacy walks study' and preparing it for publication
- Preparing three journal articles for publication
- Disseminate findings in future conferences



Social media analysis



Dr Oliver Merry
Sheffield Hallam University

A purposive search of social media platforms was conducted. Platforms included Facebook, Twitter/X, YouTube, TikTok, and Instagram. A free search for dedicated forums was also conducted. This led to a variety of social media content being examined, including 'auditor' videos, public posts, comments on police posts, and comments on videos containing police officers and/or staff. This produced a corpus of 85 potentially harmful pieces of social media content. A thematic analysis was then conducted to identify key themes.

A total of 85 potentially harmful posts and comments were identified across the reviewed sample. Following the thematic analysis, four distinct themes were identified: 'Reputation Damage', 'Personal Attack', 'Abusive Protest', and 'Identification'. In addition, seven subthemes also emerged from the reviewed content. An overview of the themes and sub-themes are presented in figure 1.

Reputation damage

This theme was characterised by attempts to damage the professional reputation of individual officers or staff. Two subthemes were identified: Defamatory Accusations and Misconduct Allegations. The defamatory accusation sub-theme involved unsubstantiated posts and comments about an individual's character and/or



motivations in a way that may undermine public trust in their position. These most commonly came in the form of paedophilia accusations towards officers involved in school-related initiatives. The second subtheme for the reputation damage theme was characterised by unsubstantiated claims of corruption from certain officers. This typically took the form of a victim or suspect who had become dissatisfied with the direction or outcome of an investigation. The officers involved in the investigation would then be targeted, attributing their disagreement with the investigative decision making with corruption and/or brutality.

Personal attack

The second theme represented the largest proportion of identified posts and comments. This theme was characterised by personal attacks and insults directed towards a specifically named, imaged, or video recorded officer or staff member. Three subthemes were identified: hostile sexism, physical presentation, and mental capacity. By far the most prevalent subtheme was hostile sexism, which was characterised by sexist comments made by seemingly male accounts towards female police professionals, typically relating to their capability, physical attractiveness, and/or sexuality. The second subtheme identified was 'physical presentation'. This subtheme included comments aimed at the physical presentation of the police officers and staff that were not of a sexual nature. These types of comments were most commonly found on 'auditor' videos and generally related to the perceived professionalism or weight. The final subtheme of the personal attack theme is mental capacity. This subtheme was characterised by insults pertaining to the officer's or staff member's intelligence or age. Similar to the physical presentation subtheme, these insults were frequently posted on auditor videos. Older officers were particularly targeted for abuse, with commenters often linking their age to age-related neurological disorders.

Abusive protest

The third theme identified within the sample of posts and comments was labelled 'abusive protest'. These comments appear to be far less targeted than the previous two themes but are characterised by generally abusive comments that demonstrate a protest to the police and their actions. Two subthemes were identified: political and rejection of authority. The political subtheme was characterised by comments and posts of anger and abuse aimed at police officers for having a perceived political bias or agenda. These were most often found in response police force account posts relating to inclusion. The second subtheme within the abusive protest theme was rejection of authority. This subtheme was characterised by generally abusive comments made to officers online. Comments within this subtheme presented with the general perception that police authority does not exist (or at least not to the same extent) online, and so the general public can use this space to express their rejection of the police.

Identification

The final theme identified within the analysis was identification. This was a less diverse theme than the others found, however it represents a real potential for harm. This theme involves the personal identification of officers and/or police staff. Virtually all videos and a significant number of images reviewed as part of the social media analysis involved the identification of officers involved. Furthermore, there was also evidence of officers being identified within the comments of videos, where their identity was not included in the video.

Managerial perspectives



Dr Shane
Horgan
*Edinburgh
Napier
University*



Dr Yen Nee
Wong
*Edinburgh
Napier
University*



Professor Liz
Aston
*Edinburgh
Napier
University*

Key activities

- Conducted 52 interviews with police managers across our partner forces.
- Reviewed 46 policy and social media guidance documents and training materials collected from both our partner forces and online sources
- Presented our findings on the importance and effectiveness of a well-being lens at the Wellbeing Conference organised by Police Scotland
- Presentation of key findings at the Edinburgh symposium and consortium
- Invited presentation at the Lancs Staff networks inspiring interesting discussions on the harms landscape, areas of online vulnerabilities and the impact of Lancs welfare policy
- Convened the first representation for the 3PO REPHRAIN lunchtime talk series, with a focus on managerial strategies in policing and the potentials for a lens of care.
- Shared project findings in a presentation for Edinburgh Napier University's Social Science seminar series.
- Presentation of findings in several academic conferences: ASC 2023, ESC 2023.
- Shared key findings and recommendations on managerial perspectives and practices through the sixth 3PO briefing series paper.

Key findings

- Primacy of preserving confidence, trust and legitimacy in organisational approaches to online risks and harms.
- Key emphasis on misconduct and individual responsibility for online personal security through a professional standards lens.
- A cultural practice of online self-regulation and the policing of peer online behaviours emerges within police organisations.
- Varied understandings of online harms among police managers inform diverse strategies around risk mitigation and harms management.
- Tendency among police managers to focus on case management and reporting, signposting and administrative processes in the management of online harms, with varied emphasis given to addressing the psycho-social and emotional impacts of experienced harms.

Recommendations

- National level advocacy for tackling online harms through key stakeholders and associated policy frameworks, underpinned by an ethics of care.
- Shifts in policy and guidance documents on online harms away from misconduct and organisational reputation towards a lens of care
- Develop an organisational culture underpinned by an ethics of care, with senior leaders championing and role modelling a well-being approach to motivate organisational change.
- Integrate online harms management into leadership training at all levels.



- Promote cross-organisation collaborations in harms management to ensure a holistic approach towards officers' online well-being.
- Channelling more resources to well-being support services to enable greater capacity for addressing online harms.

Future plans

- Further dissemination of findings within academia through presentations in large scale, international, multidisciplinary conferences. Upcoming presentations include 2 papers in ASC 2024 and 1 paper in ECREA 2024.
- Review and solidify recommendations emerging from our findings through discussions with key stakeholders in roundtable and world café events.
- Draw on our findings and recommendations to influence national level policy frameworks in partnership with key stakeholders.
- Organise roundtable sessions with our partner forces to co-produce policy documents and communications strategies relating to online harms at force level.

Police Scotland wellbeing event



Dr Shane Horgan
Edinburgh Napier University

On the 1st of February representatives from 3PO were invited to deliver the opening keynote at Police Scotland's first ever Specialist Crime Division Wellbeing Conference. 170 SCD officers and staff attended the event at the Scottish Police College at Tulliallan. Police Scotland's involvement in the 3PO the project enabled sponsorship (support? But it did pay for the catering) of the conference.

The conference ambitiously sought to showcase and raise awareness of a diverse range of contemporary issues in policing related to officer health and wellbeing and inclusion. It was opened by DCS Jordana Emerson and featured contributions from Police leaders, associations and academia across Scotland and the rest of the UK. 3POs contribution sought to highlight the project's aspirations, findings and its plans for delivering. Liz Aston, Professor of Criminology at Edinburgh Napier University and Director of the Scottish Institute for Policing Research, kicked off with an introduction to the 3PO project, (on behalf of the project lead Prof Saskia Bayerl). In her capacity as Co-Investigator on the 3PO project Liz provided an overview of the challenges facing police as public-facing professionals. She covered types of online harms identified through social media analysis and considered vulnerabilities for wellbeing from both internal and external risks. Liz highlighted ways of engaging in the project, including completing the survey which is still open and aims to provide information about the extent of online harms experienced by police in the UK. Next up were Dr Yen Nee Wong and Shane Horgan, also of Edinburgh Napier University, presenting findings on managerial perspectives on their experience operationalizing organizational policies and safeguarding their officers. Dr Marcel Obst from CENTRIC at Sheffield Hallam University demonstrated the privacy assessment tool developed by the team at centric which will enable any police officer or a family member to assess the



exposure on social media, and propose corrective action. 3PO also had a stall in the exhibition hall and was delighted to have a lot of interest from delegates coming to speak to the project team about the project and grab some 3PO merchandise.

The breadth of topics covered at this conference was exceptional, and the openness with which physical and mental health challenges experienced by police officers was striking. Numerous conversations with delegates who came to speak with us highlighted that, not too long ago, these conversations simply wouldn't have happened and that this event was truly a groundbreaking one.

Ongoing research: privacy walks to understand online behaviours and online risk prevention



Dr Marcel Obst
CENTRIC, Sheffield Hallam University

Building on the detailed interview accounts of online experiences by police personnel and their families in the previous phase of 3PO, we are now aiming to understand the way people use social media in practice. The purpose of this work is to gain a picture of privacy behaviours among police personnel and their families; for instance, how they manage visibility on concrete profiles and the reasons for choices about being more or less visible online, as well as how they experience and manage online risks to themselves or their family members. The results will ensure that the solutions 3PO builds are tailored to individuals' needs.

The approach we use is 'Online Privacy Walks'. We use mock social media profiles to encourage discussion, and speak about habits around posting, tagging, adding friends and followers, and choosing privacy settings, to name a few. Mock profiles allow us to discuss concrete behaviours and contents without having to access actual personal accounts of participants. The Privacy Walks allow us to understand perceptions of risk and privacy awareness of individuals, but also negotiations around privacy among family members.

This is ongoing work and we will be able to report findings at a later stage. However, we are already observing considerable differences in privacy behaviours and general technology literacy, for example across generations and roles.

Privacy walks

A research methodology that consists of spending time with individual participants – police officers, staff members, partners and children – to run through how they use social media. Methods like Privacy Walks, think-alouds, or scroll-backs are used to understand participants' navigation through digital platforms (Jørgensen, 2016; Robards and Lincoln 2017; Møller and Robards, 2019)¹. In these sessions, we ask participants to browse through mock social media profiles and talk through the actions they would take in relation to privacy, as well as how these profiles compare to their own social media presence.

Ongoing development: self-assessment tool to review online exposure on private accounts



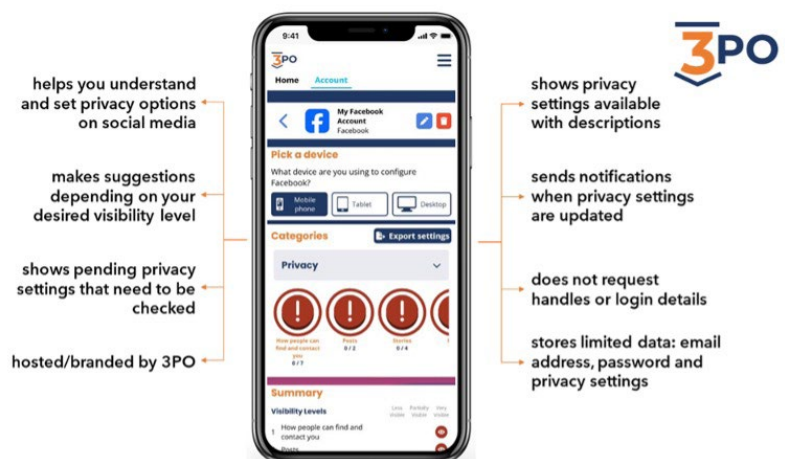
Jack Spencer
CENTRIC, Sheffield Hallam University

After conducting interviews and sessions with police officers from across the country and in various roles, we have been developing a Self-Assessment Tool that will help guide users through reviewing and assessing their privacy settings on major social media platforms.

The aim of the Self-Assessment Tool is to provide guidance about current levels of exposure and how to improve/change the amount of information accessible on personal profiles. The tool allows users to select a preference for how visible they want their profile to be, and we provide recommendations for settings based on their target visibility. We also provide a device selector, so we can customise the instructions to phone apps or desktop websites. The platforms currently supported are Facebook, Instagram, X (Twitter) and LinkedIn. These platforms were prioritised as officers we spoke to tended to have at least one of these major platforms. In future, we will work with dependents of these officers and implement platforms commonly used by younger people such as TikTok.

We demonstrated the tool to members of the public and research community during the REPHRAIN Festival of Privacy in Bristol and had very positive reactions. The tool was praised for breaking a complicated process down into simple easy-to-follow steps, and many members of the public commented on the tool's usefulness to themselves and less technically inclined family members.

Initial reactions from partners and forces have also been positive. Many praised the simple designs and user experience. At this stage, the tool is guidance-only and has no interaction with personal accounts, as many police personnel we spoke to were worried about the tool having access to their account and compromising



security. However, there was a sizeable cohort within the feedback sessions we ran who wanted the tool to have some sort of automation, where the tool integrates better into their workflow. Most of the recent development on the tool has been exploring avenues where we can deliver an experience for both sets of people, those who want no interaction with their account and those who are happy with the tool to interact with their account.

The tool supports mobile layouts from within the browser, but we realise that on mobile people use apps and like to have apps available from the home screen rather than visiting a website. In future, we want to create Android and iOS apps for the Self-Assessment Tool so that users will be able to install them from their respective app store.

Festival of Privacy - REPHRAIN



Dr Marcel Obst
CENTRIC, Sheffield Hallam University

On the 26th March 2024, Professor Saskia Bayerl, Dr Marcel Obst and Jack Spencer from CENTRIC attended the **Festival of Privacy**, a one-day event aimed at the general public for ‘fun [and] interactive sessions on how to make sense of the internet, apps and online technology’.

The Festival was organised by the National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (REPHRAIN) and the Jean Golding Institute at the University of Bristol. It took place at the M Shed, in the heart of Bristol, and was a valuable opportunity to talk with the public about the online experiences by police officers, staff and their families.

Dr Marcel Obst and Jack Spencer kicked off the day with a presentation about the 3PO project and proposed solutions for the protection of police personnel and their families, with a focus on showcasing current developments. This was followed by a discussion with a mix of members of the public, as well as members from other privacy and technology-focused projects. Discussions centred around the 3PO tool development and the potential for such tools to be extended to other public-facing professionals. Attendees also shared their own experiences, visions, and insightful thoughts on the project, helping us understand the impact that the Self-Assessment tool could have beyond its target group of police personnel.

The 3PO stall received an overwhelming response, with attendees showing particular interest in the findings and building of solutions. Whilst some visitors had been eager to visit the stall, having previously heard about the project, museum walk-ins also resulted in fascinating conversations with visitors who had never considered the topic. Repeatedly, visitors expressed that they had never thought about how police personnel, and public-facing professionals, can be victims of online harms.

At the stall, visitors had the opportunity to engage with a Self-Assessment tool prototype via three tablets and ask questions about its development and implementation, and about the project more widely. Many were sad to hear that initially the tool would not be available to the general public, and expressed how useful it would be for themselves and their own families. Attendees also engaged with a poster asking challenging and practical questions on how to safeguard police officers and staff, which further encouraged conversations on the protection of police and other public-facing professionals.



Visitor comments

Are online harms part of a police officer's job? What about their families?

Is the experience of online harms an 'inevitable' part of an officer's job – if so, should it be? My thinking is no! Families do not give their consent. In Northern Ireland, this has led to families of police officers being forced to relocate.

Yes, online harms have impact on their identities so there is a degree of responsibility on what is shared online, especially if we think about freedom of speech.

How should police officers be protected from online harms?

Human rights due diligence frameworks

They also need to be aware of not sharing personal info – PC's should have their identity protected out of work context.

How can we find a balance between freedom of speech and the protection of police officers on duty/public-facing professionals?

Capacity-building initiatives to police offices and body-worn cameras.

If we are talking about 'harassment' (perhaps online hate speech) then this is a matter re criminal law.

What could police officers/police forces/society do to protect officers online?

In Northern Ireland, for example, disguise badge numbers, only wear uniform at work, not near or from/to home. Is there an employment law reform issue.

What do you think about police officers being harassed online or having their personal details shared?

Of course police officers personal details should be protected. Regarding harassment online, low-level its part of many people's lives, but any more than that (e.g. moving offline) is not acceptable. Online harassment should be a criminal offence. There are complaint procedures in place. The crimes of harassment should be heavily punished. This falls outside the scope of their employment 'experience' – it is unacceptable.

3PO symposium - October 2023



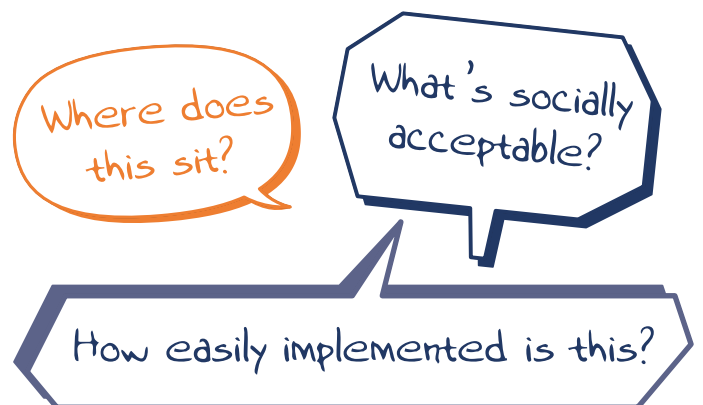
Dr Olivia Coombes
Edinburgh Napier University

On the 3rd October 2023, Edinburgh hosted the first Multi-stakeholder Symposium. With over 40 delegates attending the day began with a welcome from Professor Liz Aston from Edinburgh Napier and DCS Jordana Emerson from Police Scotland. DCS Emerson highlighted how far reaching this project is and how widespread the benefits could be.

The keynote speaker was Professor Fraser Sampson (Commissioner for the Retention and Use of Biometric Material and Surveillance Camera Commissioner) discussed the dangers facing public-facing professionals online and ran through some case studies to highlight the importance of this research. Professor Sampson presented a thought provoking visual of Mexican drug cartel Police officers wearing balaclava's and asked, "is this the future of protecting our officers?"

The day ended with an open panel discussion bringing together the expertise and experiences of Professor Fraser Sampson, Dr Shane Horgan, Inspector John Crapper and Laura Corrick.

The panel discussed and shed light on a variety of hot topics and questions from the day, such as;



As part of the day, delegates separated into tables to discuss different themes. Here is a summary of those discussions:

Youth

Difficulty in recruiting participants – although every police force collaborated with us on this project has a youth volunteer programme, recruiting children of police officers was challenging.

Self-check app – We discussed the idea of creating a self-check app that can be used as a family to help police officers and their families detect any social media risks that they might be exposed to through their online activity.

Negative experiences of children – In the symposium, we discussed some of the negative experiences children recalled during the interviews that were directly linked to their parents' policing profession. We discussed the importance of being aware of these experiences and the impact this could have on children's education and mental well-being.

Online harms and policy

Further consideration should be given to the extremely different responses female officers receive online in comparison to male officers.

Specific forces have been starting to publish misconduct findings to give clear examples and reduce more incidents. This is a very good way of providing 'real world' examples for others to learn from.

Some forces don't have any guidance on WhatsApp use within work environments, and this, as a form of social media, still needs to be highlighted more explicitly in some forces.

Technology

We prompted participants to discuss how to define risk in the frame of the Self-Assessment tool and found that there was more support for an understanding of visibility or exposure, than risk. Furthermore, participants pointed out the need to differentiate between safety and visibility/exposure.

Participants also highlighted the importance of the educational aspect of the tool, with the tool's purpose being seen as a way to learn about privacy and safety, rather than it prescribing users how they ought to handle their social media.

Participants stressed the needs for family coverage, so the tool (and training) had to be accessible and understandable for all (i.e. children and 'non tech-savvy' adults). Guidance and advice should also be made available across apps and browsers to suit every interested user.

Organisational solutions

Multi-strand approach which includes recognising the problem of online harms/risks, developing tech solutions to equip officers with abilities to manage their online activities and progression towards an understanding of online risks as a health and wellbeing issue.

Need for a well-being banner – shift towards a humane level, less heavy on policy procedure, more emphasis on protection of the self and loved-ones, responsibility of all, from individual to federation level.

Consistency is key – organisational support, cascading top-down approach, all-encompassing, both on and off duty, not about fault-finding.





World cafés - May 2024



Monica Craig
SIPR, Edinburgh Napier University

The first of three World Cafés took place in Belfast in May 2024 facilitated by Professor Liz Aston, Monica Craig, Dr Olivia Coombes and Dr Lasara Kariyawasam. World Café methodology is a simple, effective, and flexible format for hosting large group dialogue. The aim of this session was to engage representatives from Police Service Northern Ireland (PSNI) in a structured conversational process which allowed for open discussion and knowledge exchange.

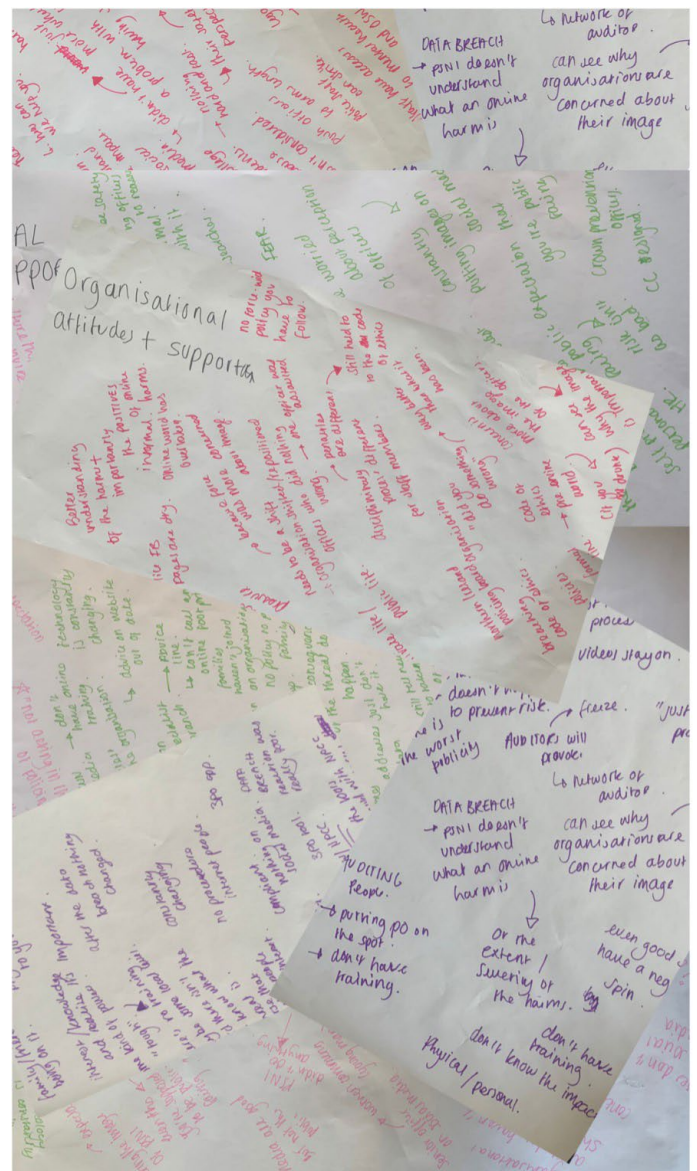
There was good attendance at the event with approximately 30 participants engaging in the session, representing policing staff and officers across several roles, ranks and departments. Working with key organisers from PSNI, facilitators divided participants into four groups accounting for rank and seniority where possible.

The world café focused on four themes.

1. Creating better knowledge about online harms;
2. Addressing disparate risk profiles and needs;
3. Organisational attitudes and support; and
4. Prevention and protection solutions for individuals, families, and forces.

Participants were welcoming of the concept and aims of the 3PO project. It was felt that finding could help organisations to have a better understanding about online harms. These discussions identified core issues in the current approaches to dealing with online harms, in particular, a need to better define what 'online harms' are, along with recognition of their impact.

Overwhelmingly, feedback indicated that police staff and officers did not feel there were sufficient processes, policies, nor guidance in place to help staff and officers navigate these issues. Furthermore, it was felt that the culture in most forces does not support staff and officers to recognise or report these harms with the emphasis being placed on protecting the organisational reputation over individual health and wellbeing. It was felt that





these is an over reliance on 'common sense' as well as an expectation that online harms were just 'part of the job'.

Furthermore, it was felt that current social media policies are not realistic promoting restrictive use as opposed to guidelines. This can result in policies being reactive rather than proactive/ preventative.

Impacts on families and dependents were detailed including how partners and spouses are heavily relied on for digital engagement, and children often not being aware of what their parents do for a living.

Participants were welcome to the concept of training and tools developed from the 3PO project. It was felt that these should be something available to all forces. Discussions pointed to a need for safe environments where issues can be reported free of judgement and stigma, and which are victim centred There also needs to be clear reporting guidance, which is not only realistic, but which also accounts for individual differences gender, cultural, community, or belief systems.

Furthermore, there needs to be recognition of not only the different local needs met by each police force, but also the different risks faced by diverse staff and officer roles with those based in neighbourhood/ community policing roles felt to be most at risk. This would help 'future proof' forces, particularly as recruitment aims to engage with younger generations as well as potential staff from diverse backgrounds. In addition to supporting staff and officers, participants also felt that it was important to have stronger legislations and punishments for those who intentionally harm police officers and families. In order for this training to be delivered, it was recommended that more 'interactive' sessions (e.g., the world café) would be preferable over just providing documents. For children this might involve the development of child friendly 'game-like' tools to create awareness.

Publications

Over the course of the year, the 3PO Project have published a number of reports and briefing papers, which you can find here:

[Christmann, K, Becker, I. \(2024\). Specialist Officers.](#)

[3PO Project Members, \(2023\). 3PO Summary Report: Overview of Initial Findings.](#)

[Merry O, \(2024\). 3PO: Social Media Analysis.](#)

[Bates A, Whitfield K. \(2024\). Interview with Police Officers/ Staff and Partners.](#)

[Kariyawasam L, Mueller-Johnson K. \(2024\). How Children of Police Officers Keep Safe Online.](#)

[Bayerl S, Akhgar B, Obst M, Snowden M, Spencer J. \(2024\). Co-Developing Technological Solutions.](#)

[Wong N, Y, Horgan S, Aston L, \(2024\). Managerial So...](#)



Presentations

Project members have presented 3PO at the following conferences:

- British Psychological Society's Cyberpsychology conference
- Refrain All Hands Meeting
- Thames Valley Police Conference
- Family Liaison Officers' conference
- Police Scotland Specialist Crime Division Wellbeing Event
- Refrain Conference
- Lancaster Security Seminar
- European Society of Criminology
- American Society of Criminology Conference
- REPHRAIN Lunchtime talks
- High-level Knowledge and Policy Exchange DG Home
- REPHRAIN Festival of Privacy
- Security and Policing 2023

Information

[re]Searchlight

In February 2024, The Scottish Institute for Policing Research launched the first episode of their brand new podcast [re]Searchlight.

The first episode features an in-depth discussion with Dr Oliver Merry from Sheffield Hallam University. Dr Merry is a senior lecturer in Forensic Psychology and a researcher on the 3PO Project.

Dr Merry led a 'social media analysis' (see page 12) which looked into the real social media harms aimed at police officers, finding that these online harms tend to fall into one of four categories: reputation damage, personal attack, abusive protest and identification.



