SCOTTISH POLICE
AUTHORITY
ÙGHDARRAS POILIS NA H-ALBA

OFFICIAL: POLICE AND PARTNERS

# Horizon Scanning Report

## Futures in Policing

4th Edition

2025

# Contents

Horizon Scan - 4th edition

1. Contents & Introduction - pg. 2

2. A Cashless Future? - pg. 3

3. Sharenting - pg. 5

# Introduction

## What is horizon scanning?

The Scottish Police Authority ('The Authority') regularly reviews a range of sources (including news briefings, research and reports) to identify emerging areas of interest that could impact policing and the wider justice sector. This is known as 'horizon scanning' and is a process used by many organisations in the early discovery of emergent issues.

This review process is used to form our 'knowledge bank', where issues related to the current and future work of the Authority can be identified. Topics are analysed in more depth within regular horizon scan reports, with potential implications for policing and the wider sector drawn out.

It must be emphasised that these reports are speculative in nature and any implications are derived following analysis of evidence by Authority Staff. Readers are encouraged to access referenced sources using the hyperlinks embedded throughout this report. Please note that the viewpoints included in this report do not necessarily reflect those of the Authority.

The report will continue to evolve with time and following feedback from recipients. Please direct any feedback or responses to: SPAStrategyandPerformance@spa.police.uk

# A Cashless Future?

**Key Terms**: Digital, Fraud

**Last updated**: January 2025

**Estimated impact on policing and justice system**: Medium

**Estimated timescale**: Long term

## Summary

Across the globe, different countries are seeing a rise in cashless payments. Scandinavian countries are at the cutting edge of cashless payments. 3 to 4 per cent of transactions use notes or coins within Norway.

India has sought to prioritise digital payments through a government-led Unified Payments Interface (UPI), which has led to a variable impact on the decline of cash in the long-term. China also has advanced digital payment options in its increasingly cashless society, that integrate a variety of transactions and advanced biometric capabilities. However, this has been slowed to ensure the inclusion of all in its economy.

From a UK perspective, HM Treasury did not order new coins in July 2025 from the Royal Mint, reflective of the decline in the use of cash in the UK. In addition, the Bank of England are considering the case for a digital pound to be used alongside cash.

UK Finance research has shown that 39% of adults live an almost cashless life. As well as predicting that cash payments in the UK will continue to decline, and that by 2031, cash will account for 6% of all payments. This reduction in the usage of cash is also reflected in the planned closure of 23,000 cash machines by 2030. However, research has shown that during the cost-of-living crisis, those using cash on a regular basis was at a four year high.

The use of cash also varies by generation. 42% of people aged 85+ say that they rely on cash to a great or very great extent, however 72% of those aged 16-24 regularly use mobile payments. In addition, those with a low household income (less than £15,000 annually) are almost three times more likely to rely on cash. Research has also found an increased reliance on cash for those in poor health, or those who are unemployed. Digital exclusion also has implications for cash reliance, with 46% of those classed as digitally excluded (defined as those who have limited abilities to use the ability and who rarely use it) relying on cash.

> “39% of adults live an almost cashless life”

Recognising the potential challenge that could be faced by different areas of the population, the Financial Conduct Authority established rules in September 2024 to ensure that communities across the UK have reasonable access to cash. This would require banks and building societies to maintain the position that 95% of people living in an urban area being within one mile of a cash access point, and people living in rural areas being within three miles of a cash access point.

### Implications for policing and the wider justice system

Cashless societies may present benefits to the wider public, particularly as digital payments also enable greater economic transparency. It has been predicted that some types of theft and robbery may be reduced. However as individuals rely on mobile devices to make payments, decreases in some forms of theft could be contrasted with the increase in other forms of theft. So-called “snatch thefts” (where an individual’s mobile phone or handbag is stolen from them on the steet) more than doubled in the year ending June 2024 in England and Wales. This has led to the UK government pledging to reduce the number of phone thefts.

However, as digital payment methods are susceptible to hacking, this may present risks to individuals

# A Cashless Future? (continued)

and businesses if relied upon as a sole access point to money. Recognising the disproportionate impact of online fraud on vulnerable people, multi-agency initiatives such as The Banking Protocol aim to identify potential victims of online fraud early. In Quarter 1 of the 2024/25 reporting year, over £1million worth of fraud funds was prevented.

In addition, a more cashless society requires a reliance on infrastructure and underpinning technology. However, this may leave individuals and wider society vulnerable to any technological or infrastructure failures.

As previously discussed, as some facets of society are excluded, this may have sociological implications and a compounding of exclusion. However some argue that cashless societies can help to support "unbanked" individuals, for example those who may live in more rural areas who have limited access to traditional banking methods.

In addition, some also raise concerns on privacy implications as digital transactions increase, suggesting that options for pseudonymised data be explored. Pseudonymised data is data which has been processed so that it cannot be attributed to a specific person.

Cash payments are anonymous and are therefore challenging to trace.
Criminals may therefore seek alternative methods as the use of cash declines. For example, artificial intelligence (AI), crypto-currencies, the dark web and gambling can be used as methods to evade tracing by the police via money laundering. Using AI large language models, alongside phishing and ransomware-as-a-service models, criminals can create sophisticated and targeted attacks.

Tackling crimes related to cryptocurrency can often present a challenge to policing. Cryptocurrency can enable prompt, anonymous financial transfers across the globe and can be challenging to police. Interpol note that tackling this requires "sustained and concerted action" of policing, alongside partners and regulators. However, research has shown that often criminals accept smaller scale payment through legitimate bank accounts, obscuring criminal activity.

Banks have already employed AI to detect fraudulent transactions to intercept scams. As some police forces have demonstrated partnership working with private sector organisations for other financial crimes, it will likely be important to enhance such partnership working throughout policing in the future. This will allow policing to implement advanced technologies developed by partners to monitor, detect and pursue crimes.

In addition, as smaller scale transactions have permeated into legitimate banking mechanisms, this will require sophisticated algorithms to detect such crimes. This deviation from predictable illegal behaviour, conducted through digitally hybrid means, will present a challenge to policing to address. Policing may wish to consider proactive methods of identifying future digital payment approaches that may be used for illicit activities.

Policing's focus on monitoring, detecting and reacting to crime and could arguably be evidenced Police Scotland's recently published three-year business plan. This includes a commitment "Invest in capabilities outlined within our Policing in a Digital World workstreams to better prevent, protect, prepare and pursue cyber-crime, including joining the fraud and cybercrime reporting and analysis service".

To ensure that any future developments towards an increasingly cashless society are carefully managed, some have called for robust financial regulatory frameworks to protect individuals. Such frameworks would allow banking institutions and wider society to be held to standards and protocols to protect consumers and organisations. However, it will be important to ensure that any framework or policy developments are futureproofed to ensure they are fit for purpose as technology continues to emerge.

# Sharenting

**Key Terms**: Children and young people; technology

**Last updated**: January 2025

**Estimated impact on policing and justice system**: High

**Estimated timescale**: Short term

## Summary

"Sharenting" refers to the practice of parents sharing information, photos, and videos of their children on social media. Sharenting encompasses various online behaviours, including sharing milestones, day-to-day activities, and sensitive information about children.

While this trend has become prevalent in the digital age, it raises significant ethical and legal concerns, particularly in relation to privacy, consent, and an infringement of children's rights. The negative outcomes associated with sharenting has resulted in researchers calling for improved regulation by social media companies with regards to sharenting.

Since children cannot provide informed consent about their online presence, the ethical implications of parents sharing personal information become increasingly significant. Research has found that children aged 10 to 17 do not wish their parents share personal information, or content which they find embarrassing.

Sharenting can also have long-term repercussions on children's mental health, with research also suggesting that it can result in an increased risk of children experiencing online bullying and exploitation.

Human Rights Watch has raised concerns around the use of Artificial Intelligence (AI) in using images of children to create deep fakes, and the information relating to children that can be uncovered by AI through images posted of them online.

The risks relating to sharing information online has resulted in the introduction of the Children's Image Rights Law in France. This legislation provides children with digital rights, which includes the right of access, rectification or erasure in relation to their personal data.

Whilst recognising the impact of sharenting on the lives of children and young people, their safety and wellbeing may also be impacted by their use of the internet. The Internet Watch Foundation found that children under ten are being increasingly targeted by groomers and have reported a "record amount of child sexual abuse". The Foundation has also found an increase in the sexual extortion (or "sextortion") of children and young people online, with an increase of 19% in the first six months of 2023 compared to 2024.

### Implications for policing and the wider justice system

Sharenting presents complex challenges for policing and the Criminal Justice system in Scotland and the UK. As this phenomenon evolves, legal frameworks and policing strategies must be adapted to ensure the protection of children's welfare while navigating the digital landscape.

In Scotland, safeguarding children's personal information is a paramount concern, reflecting a

# Sharenting (continued)

commitment to protecting their privacy and well-being.  A focus on safeguarding will helps to prevent potential risks associated with data breaches or misuse will also promote a culture of trust among families and communities regarding the protection of children's rights in the digital age.

Sharenting may bring new challenges for policing, particularly concerning cybercrime and child exploitation. The practice can inadvertently expose children to risks such as online predation and cyberbullying, necessitating proactive responses from Police Forces.

Police Officers are increasingly required to monitor social media for potential threats, while posts can also serve as crucial evidence in investigations of harassment and exploitation.  Whilst addressing online child exploitation has continued to be a priority for policing at some time, the utilisation of images posted by the families of children by criminals requires proactive and innovative approaches. As investigations will further be complicated by the vast volume of online content, this will make it challenging to identify harmful posts amid the extensive shared information. This complexity requires sophisticated technologies and methods.

Policing may therefore consider different approaches to mitigate the negative impacts of sharenting. First, increasing public awareness through educational initiatives focused on the risks associated with sharenting is essential. Emphasising privacy, consent, and the implications of a digital footprint can empower parents to make informed choices. Policing may have to allocate resources to inform parents about the risks associated with sharenting, focusing on digital literacy and child safety. This could, for example, include encouraging parents to discuss any information they plan to share of their children online with children themselves prior to posting on social media. This could be influenced by future research looking to specifically address harmful sharenting practice, with some research finding that showing parents a video highlighting the dangers of sharenting results in a "significant proportion" being less willing to share images of their children.

> " Sharenting can also have long-term repercussions on children's mental health"

Sharenting also raises important legal considerations within the Criminal Justice framework. Existing privacy laws in the UK, such as the Data Protection Act 2018, provide a foundation for addressing the issues arising from sharenting, but the application of these laws can be ambiguous, particularly when it comes to parental consent and children's rights. Therefore, there is a need for policy development to establish clear guidelines for Police Forces and the Criminal Justice system in handling sharenting-related cases. Consistency in addressing these issues will help protect children's rights and welfare.

Police Scotland has previously had an inspection of its response to online child sexual abuse completed by HM Inspectorate of Constabulary Scotland in 2020. Police Scotland reported the closure of all but one action in December 2024.

However, changes in technology such as the use of AI in online child sexual abuse cases present a growing challenge in the safeguarding of children. It will be important for policing to work alongside technology companies to work in collaboration and sharing information and resources. Whilst legislation such as the Online Safety Act 2023 has been implemented with a focus on protecting children and young people, it will be important for organisations to continually assess emerging threats that may not be covered by legislation.

Finally, fostering collaboration between the Police, Social Services, and educational institutions can create a more unified approach to addressing the implications of sharenting. This inter-agency cooperation is crucial for effectively navigating the challenges posed by the digital age.

Through education, policy reform, and inter-agency collaboration, the negative impacts of sharenting can be mitigated, fostering a safer online environment for future generations.