HEDDLU
GOGLEDD CYMRU
NORTH WALES
POLICE

Response Date:16/09/2025

2025/962 - Use of Mobile Phone Data Extraction

In response to your recent request for information regarding;

1. **Does your police force currently carry out mobile phone data extraction in low level crime cases using self-service / downloading kiosks? Please provide your definition of low-level crime.**

   No

2. **Does your police force currently carry out mobile phone data extraction in serious crimes using self-service / downloading kiosks?**

   No

3. **If your police force is not currently using mobile phone extraction kiosks, have you trialled this in the past/do you have plans to in the future?**

   Yes, NWP previously had touch devices out on division, with the roll out of ISO accreditation, data management and cost this model was seen and prohibitive so it was re-centralised in 2015-2016.

   No immediate plans to go in this direction again.

4. **Does your police force currently use Hubs to carry out mobile phone data extraction in (a) low-level crimes? (b) serious crimes?**

   No

5. **Do you centrally record mobile phone data extracted from kiosks?**

   N/A

6. **If you have a mobile phone extraction kiosk, please provide the name of the company(ies) which currently provide(s) the hardware / software / to whom you pay a license for the relevant tools. If contracts for these tools exist, please also provide the beginning and end dates of these.**

   N/A

7. Does your police force use analytics software to process, analyse or evaluate data extracted from mobile phones? If so, please provide the name of the software or provider.

Yes.

Concerns have been raised in relation to providing the names of digital forensic laboratories and/or outside forensic science services used. Therefore, a public Interest Test has been carried out to weigh up the reasons for and against disclosure; to ensure the release is in the interest of the public as a whole and not just the applicant.

Section s31(1)(a)(b) Law Enforcement

Section 31 (1)(a)(b) is a prejudice based qualified exemption, therefore there is a requirement to articulate the harm that would be caused in confirming or not that the information is held as well as carrying out a public interest test.

The Harm Test process requires North Wales Police to consider any possible harm that might arise as a result of placing the requested information into the public domain. This process considers the potential harm to:

- Individuals
- The community as a whole
- North Wales Policeand the wider policing service
- Other bodies

Policing is an information-led activity, and information assurance (which includes information security) is fundamental to how the Police Service manages the challenges faced. In order to comply with statutory requirements, the College of Policing Authorised Professional Practice for Information Assurance has been put in place to ensure the delivery of core operational policing by providing appropriate and consistent protection for the information assets of member organisations, see below link:

https://www.app.college.police.uk/app-content/information-management/

Commercial Forensic Service Providers are vitally important in the Criminal Justice system - not only do they play a crucial role by supporting UK Policing with backlogs in the Digital Forensics arena, but they provide Defence teams with access to independent forensic experts to support their clients.

Whilst not in any way questioning the motives of the applicant, it must be taken into account when considering potential harm that a disclosure under the Freedom of Information Act 2000 is made to the world at large, rather than a private correspondence. Specific details of any forensic service providers used by North Wales Police would be extremely useful to those involved in criminality as it would enable them to create a map of those most used by police Forces. Forensic Service Providers can be targeted by malicious actors, for example in 2019 Eurofins (one of the UKs largest FSPs) suffered a highly sophisticated ransomware attack which severely disrupted UK Policing and the Criminal Justice system.

https://www.helpnetsecurity.com/2019/06/24/eurofins-ransomware-attack/
https://www.theguardian.com/science/2019/jul/05/eurofins-ransomware-attack-hacked-forensic-provider-pays-ransom

By providing a list of forensic service providers, Force by Force, a malign individual could identify those most critical to the Law-and-Order sector and specifically target those proving the most assistance. This would have a huge impact on the effective delivery of operational law enforcement as it would leave companies open to further cyberattacks which could have devastating consequences for law enforcement.

Factors favouring Disclosure
Confirming the names of Forensic Service Providers would be of interest to the public, namely give insight into the forensic processes used to solve crimes.

Factors favouring Non-Disclosure
Measures are put in place to protect the community we serve and as evidenced within the harm, to provide a detailed list of Forensic Service Providers would allow individuals intent on disrupting law enforcement to target specific companies using the information obtained to maximise the impact.

Taking into account the current security climate within the United Kingdom, and the Eurofins cyber-attack, no information which may aid criminality should be disclosed. It is clear that it would have an impact on a Force's ability to carry out the core duty of enforcing the law and serving the community.

The public entrust the Police Service to make appropriate decisions with regard to their safety and protection and the only way of reducing risk is to be cautious with what is placed into the public domain.

Balance Test
The Police Service is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. In order to effectively and robustly carry out those duties, external services are utilised which are vital to investigating criminal activity. Weakening the mechanisms used to investigate any type of criminal activity would have a detrimental impact on law enforcement as a whole. To provide the names of the FSPs despite the known risks of cyber-attacks would undermine any trust or confidence the public have in the Police Service. Therefore, at this moment in time, it is our opinion that the balance test favours against the disclosure of the FSP used for digital forensics.

In accordance with the Freedom of Information Act 2000, this letter acts as a Refusal Notice under section 17 (1) of the legislation.

8. **How many officers currently carry mobile phone examination kits on patrol and/or in vehicles and/or for other operational use in (a) low level crimes? (b) serious crimes?**

   None

9. **Please confirm whether or not a review has been conducted into the use of self-service kiosks.**

   No

10. **Please provide copies of the current relevant force level and/or national level guidance for the use of downloading kiosks.**

    N/A

11. **Please provide copies of the current relevant force level and/or national level policy for the use of downloading kiosks.**

    N/A

THIS INFORMATION HAS BEEN PROVIDED IN RESPONSE TO A REQUEST UNDER THE FREEDOM OF INFORMATION ACT 2000, AND IS CORRECT AS AT 16/09/2025