Social media as digital evidence. The impact and access challenges in modern drug police investigations.

https://github.com/maria0904m/Final-Year-Project---COMP3000.git

Project Vision

This research based project is designed for law enforcement agencies who face increasing challenges in accessing and investigating social media during criminal investigations. This research also has the purpose of raising awareness of the importance of digital evidence in modern policing, as most crimes now have to an extent a form of digital activity. According to His Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS, 2023) "Most crimes today have a digital footprint – a trail of data that is left behind by users of digital services. And electronic evidence (found on computers, smartphones, remote storage, smart devices and more) is part of almost all criminal activities.". This highlights the growing significance of digital forensics and the urgent need for efficient frameworks to ensure legal and ethical access to online evidence during investigations.

This research will critically analyze how investigation of social media platforms could influence the investigation process and court outcome. It will look at the methodology of management and handling digital evidence of a police force to ensure continuity of evidence and the difficulties met by law enforcement when the case has a digital footprint.

The research aims to identify and analyse the legal, technical and ethical barriers that impede the effective access to social media information, access the effect of these barriers to the effectiveness of modern policing investigations, examine collection of digital evidence methodology and propose recommendations for improving lawful data collection, agencies collaboration and evidence management processes within the boundaries of data privacy and legislation.

Risk Plan

1. Data sensitivity and confidentiality

The project involves working with anonymised police case studies to explore how personal social media platforms influence drug investigations. There is a potential risk that case information could include sensitive operational details or identifiers related to past investigations.

To mitigate this all data provided by law enforcement will be anonymised prior to receipt with no personal names, case numbers or identifiable information. Data will be stored securely and will be accessed from a police computer, which will be protected and stored under law

enforcement policy and will be accessible only to the researcher and relevant law enforcement parties. No one will have access to editing these files, to protect the integrity of data within the documents. The case studies will not be transmitted to any other party or viewed on any other different devices, but a police computer. All materials will be permanently deleted after assessment submission, in compliance with GDPR.
Findings will only be presented in aggregated or generalised form, ensuring that no specific case or individual can be identified. To further protect the integrity of data used in the research, the full version of the study will not be publicly published, and will be privately archived. In the event that the research is later considered for public release, a generalised redacted version will be created, to ensure that operational, confidential or sensitive data will be fully removed.

2. Access and feasibility risks

Obtaining anonymised case summaries represent a key feasibility risk. Police availability and legal clearance may limit the depth or quantity of case data shared, potentially affecting the scope of the study. This will be mitigated by early engagement with police contacts and flexibility in research design. If the access is delayed or totally restricted, the study will look instead at secondary data sources, such as open access police reports, published case summaries and official Home Office documents. This will ensure that in the absence of primary case data, the project retains analytical depths and relevance.

(To maintain research continuity, communication with law enforcement will follow a clear timeline, and all communication will be conducted via official channels)

3. Research bias and interpretation risk

Qualitative research by definition involves interpretative analysis, which can introduce subjective bias. The risk is in emphasizing certain narratives, particularly those which support the researcher's assumption about the law enforcement matters.
To minimize this , the study will adopt a reflective approach, maintaining a reflective research approach, to document decision, assumption and potential bias throughout the project lifecycle. Comparing police provided insights with academic literature and public data is a key element to ensure balanced conclusions. Supervisor review will be used as a further validation check to ensure objectivity.

4. Time management

Given the dependency on external data from law enforcement, delays are likely to disrupt the project timeline. To mitigate this, contingency time frames for possible delays in receiving case studies or ethics clearances are included in the project schedule. Case study analysis is planned toward the later stages of the research, providing additional time to accommodate any unforeseen delays. A fortnightly milestone using a Trello board will track progress, backed up by regular sprint meetings with the supervisor to ensure alignment with deadlines. In case of significant delays, the literature review will be prolonged and supplemented by available public reports to preserve analytical momentum and continue and generate meaningful insights.

5. Reputational and communication risk

Engagement with a police institution requires professional conduct and precise communication. Miscommunication or informal handling of requests could risk reputational damage or misunderstanding regarding research aims. To avoid this, all communication with the police force will be formally worded, documented and conducted via official channels, following their instructions, ensuring professional transparency and accountability without compromising credibility to any parties.

6. Technology and platform risk

Social media platforms regularly update their terms and conditions, privacy policy and technical structures. These changes can affect the applicability or relevance of case studies, particularly when investigating procedural access to digital evidence. The danger is having conclusions that quickly can become outdated or misaligned with operational facts. To mitigate this, the research will adopt a conceptual approach with a general solution to issues and legal or technical problems rather than platform specific operational methods. Additionally, the literature review will include discussion of policy evolution and technological trends so will be assured that the results do not lose relevance with the ongoing platform changes.

7. Scope Creep

Considering the exploratory nature of this research and personal passion for this topic, there is a high risk of scope creep, in which the project expands beyond its original objective. If left unguided and unsupervised, this would compromise the project's focus and lead to overwork. To prevent this, I will strictly adhere to original research questions and purpose, having in mind the aims of the project. Constant tracking of progress via trello board and sprint meetings with the supervisor will keep this project on track, within bounds, and within its intended aims.

8. Researcher wellbeing

This research involves heavy literature review, qualitative case study analysis, which may lead to undue workload and stress considering the ethical matters involved within the subject. The long duration of focused research or waiting for case information may negatively impact the health and productivity of the researcher. To avoid this, the project will be well structured, with key milestones, time management and supervisor meetings and guidance.

LESP

Legal constraints and risks

This research operates within a complex legal and regulatory framework that governs digital evidence, digital materials and law enforcement access to individual social media platforms. Relevant legislation includes Data Protection Act 2018, General Data Protection Regulation (GDPR), Investigatory Powers Act 2016, Computer Misuse Act 1990 and the Human Rights Act 1998 (Article 8). These laws govern the collection, storage, examination and use of digital data, subjecting it to complex requirements of privacy and legal access.

The principal ethical risk is risk of confidentiality violation through unintentional disclosure of sensitive information, or inclusion of law enforcement techniques that compromise operational security

Important legal risks are misinterpretation or misuse of law that could result in legally non compliant conclusions or recommendations. For instance, examination of police access to encrypted or private social media messages might unintentionally suggest methods non compliant to UK law.

Mitigation strategies are:

- Conducting research only using anonymised case study data.
- Focusing on conceptual and procedural analysis rather than operational instructions.
- Framing all findings within the current UK legislation and laws.
- Adhering to relevant laws when conducting the research
- Interaction with the police force will be adequately documented.

Ethical constraints and risks

The project involves ethically sensitive topics, including drug crimes, social media use, and surveillance online. Moral issues are unintentional disclosure of identifiable facts, distortions of policing practices, or speculation that would have an impact on public trust and operational integrity.

Mitigation strategies are:

- Obtain university ethics consent prior to analysis
- Conducting research only using anonymised case study data.
- Prevent access to raw social media materials, personal data, or confidential communications
- Informed consent for optional police interviews, and allow participants to withdraw any time, if applicable
- Apply the ethical principle of minimisation, only using data necessary to answer the research questions

Social constraints and risks

The project raises social issues like privacy, digital rights and public opinion of policing. A risk exists where results are misrepresented or misinterpreted, leading to a negative public perception of the law enforcement operational duties or social media platforms. Discussing digital surveillance or access challenges could raise societal concerns about digital privacy.

Mitigation strategies are:

- Report research results only using anonymised case study data.
- Summarize conclusion in academic literature and public policy, with attention to legal and ethical constraints.
- Avoid assumptions about individuals or policing procedures.
- Clarify the purpose of the research as an analysis of the systematic problems, rather than operational critique of law enforcement.

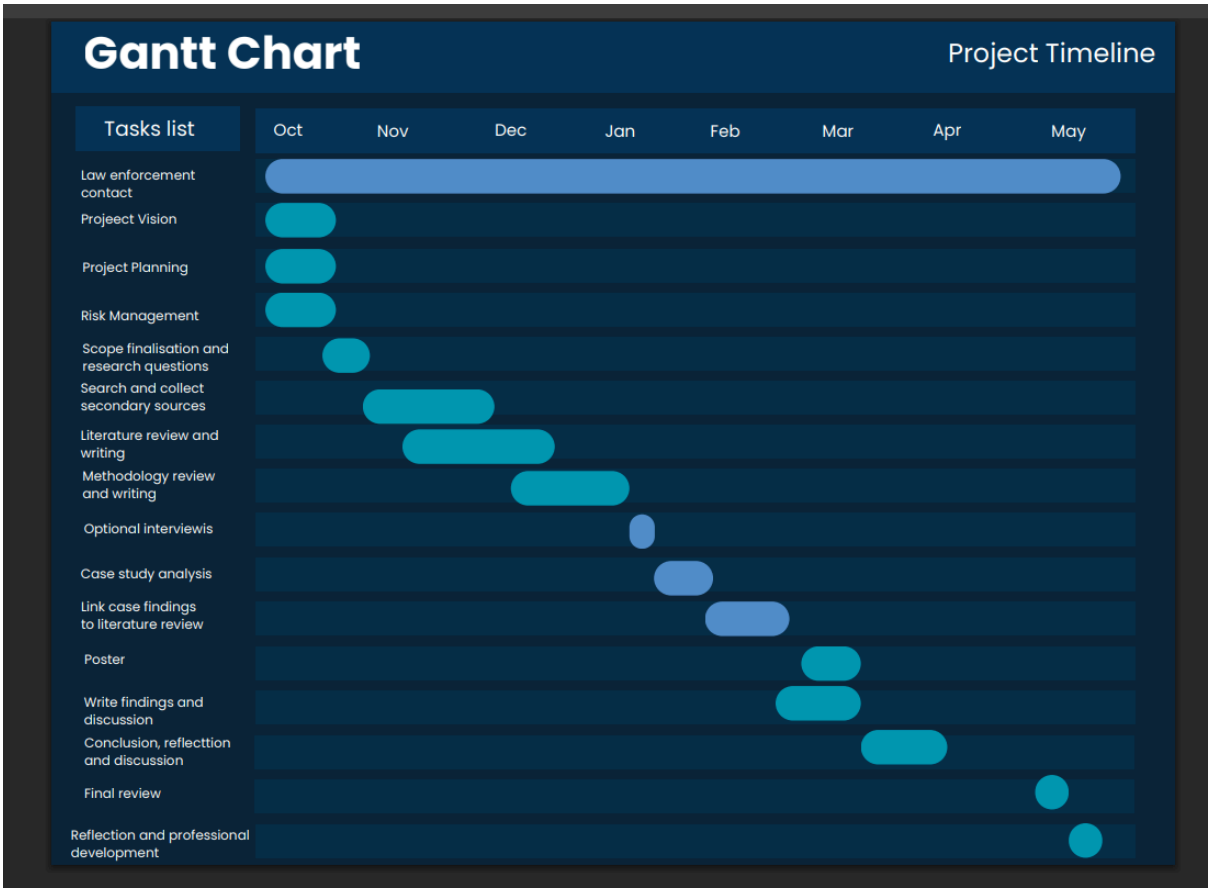
Professional constraints and risks

These risks relate to research integrity, communication with the police force and adherence to academic standards. Miscommunication with police contact, misunderstanding of procedures or absence of data protection protocols may damage both researcher credibility and professional collaboration with third party partners.

Mitigation strategies are:

- Formal, documented (where possible) communication with police force
- All findings evidence based and relevantly documented
- Follow university research best practices in regards to data handling, referencing and ethics.
- Hold regular meeting with supervisor to review methodology, progress, and analysis of results
- Using project management tools

Gantt Chart



Reference List

- Data Protection Act 2018. (2018). UK Public General Acts. [online] Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted [Accessed 21 Oct. 2025].
- General Data Protection Regulation (GDPR). (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council. [online] Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj [Accessed 21 Oct. 2025].
- His Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS). (2023). Digital crime and policing. [online] Available at: https://hmicfrs.justiceinspectorates.gov.uk/our-work/article/digital-crime-and-policing [Accessed 21 Oct. 2025].
- Human Rights Act 1998. (1998). UK Public General Acts. [online] Available at: https://www.legislation.gov.uk/ukpga/1998/42/contents [Accessed 21 Oct. 2025].
- Investigatory Powers Act 2016. (2016). UK Public General Acts. [online] Available at: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted [Accessed 21 Oct. 2025].
- Parliamentary Office of Science and Technology (POST). (2022). Use of digital, scientific and other technologies by the police and wider criminal justice system. UK Parliament. [online] Available at: https://post.parliament.uk/use-of-digital-scientific-and-other-technologies-by-the-police-and-wider-criminal-justice-system/ [Accessed 21 Oct. 2025].
- The Computer Misuse Act 1990. (1990). UK Public General Acts. [online] Available at: https://www.legislation.gov.uk/ukpga/1990/18/contents [Accessed 21 Oct. 2025].
- Canva. (2025). Canva [online design platform]. Available at: https://www.canva.com [Accessed 23 Oct. 2025].
- Monday.com. (2025). Monday.com [online project management tool]. Available at: https://monday.com [Accessed 23 Oct. 2025].