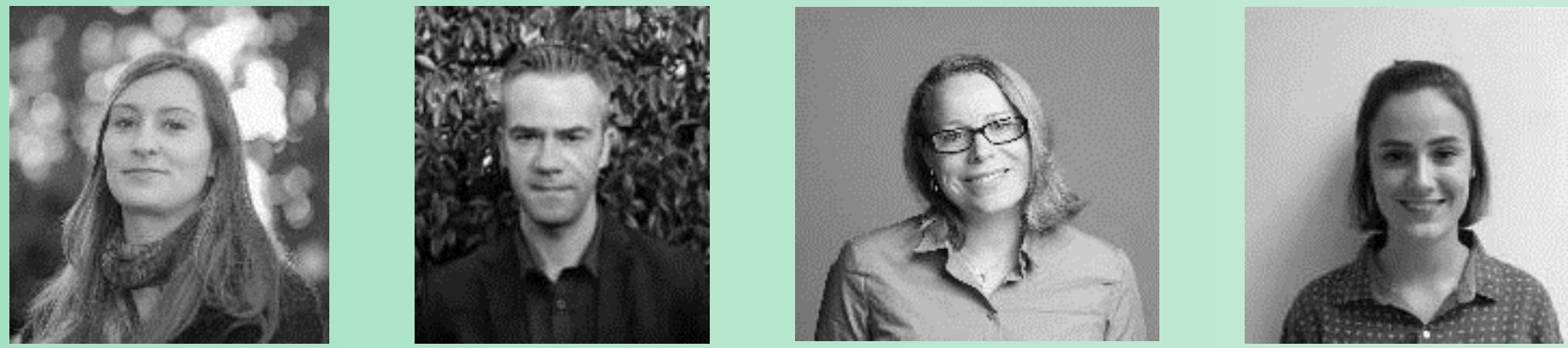


# UK Computer Misuse Act 1990 & Technology-Enabled Domestic Violence/Abuse



Leonie Tanczer, University College London (*Tech Abuse*)  
 Shane D Johnson, University College London (*Policing*)  
 Frances Ridout, Queen Mary University of London (*Law*)  
 Francesca Stevens, City/University of London (*Victimisation*)



## Background

- **Focus:** The applicability of the UK Computer Misuse Act 1990 for cases of technology-enabled domestic violence and abuse (“tech abuse”)
- **Tech Abuse:** A “big bucket” – across systems – includes:
  - Excessive text messaging
  - The use of malicious software so-called “stalker-/spyware”
  - The deployment of (car) trackers
  - The impersonation of an individual
  - Image-based abuse offenses
  - Unauthorised access to accounts/devices/systems
- **Prevalence:** National Stalking Helpline says 100% of cases involve a “cyber” element



## Legal Dimension

- Tech abuse: Not a **domestic abuse/stalking offence** *per se*
- **Common Legislation:**
  - Criminal Justice Act 1988
  - Protection of Harassment Act 1997
  - The Serious Crime Act 2015
  - Criminal Damage Act 1971
  - Public Order Act 1986
- **Activities such as hacking** into someone’s phone or installing malicious software can fall under the UK Computer Misuse Act 1990
  - 5 Criminal Offences – Focused on “Unauthorised Acts/Access”



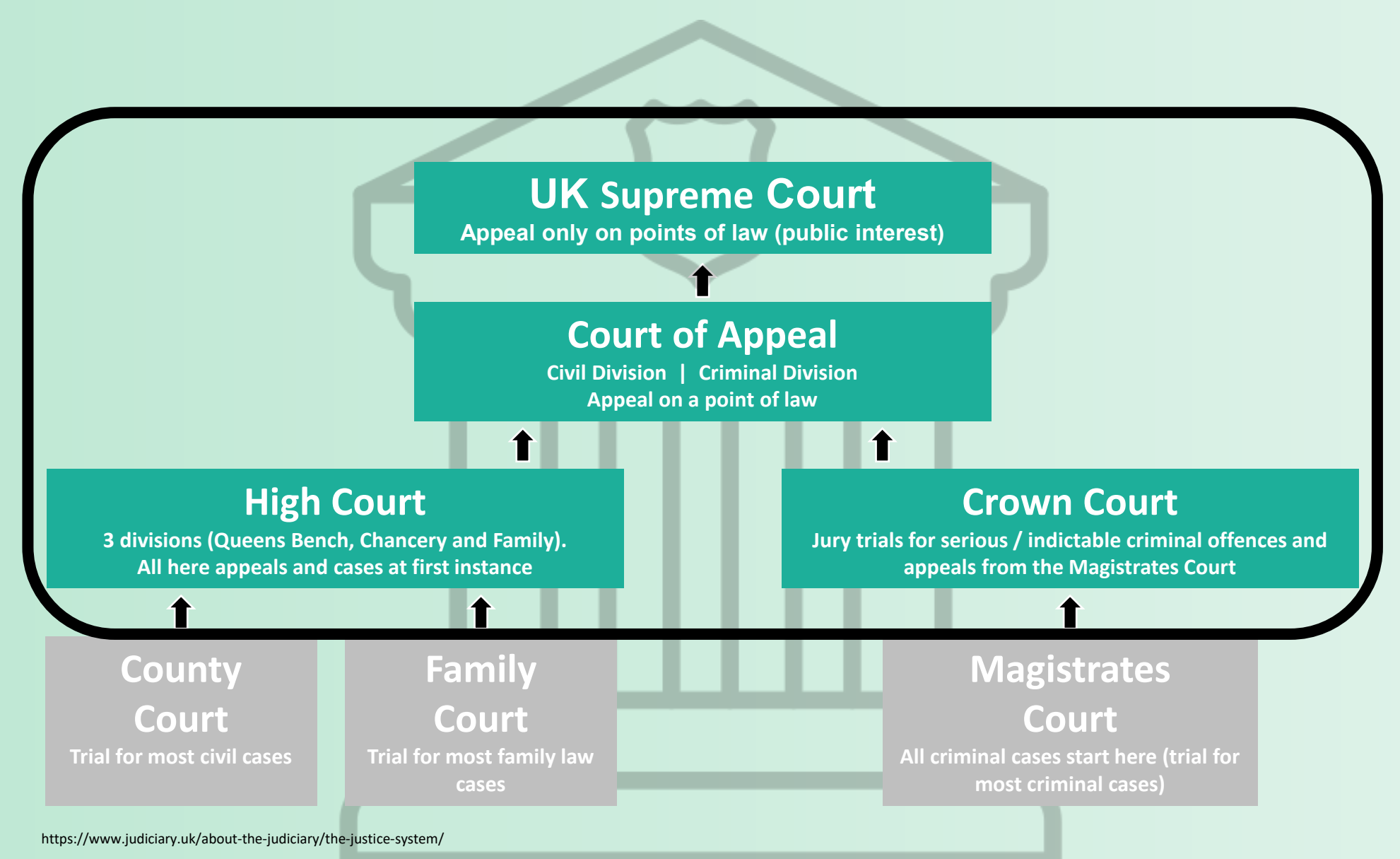
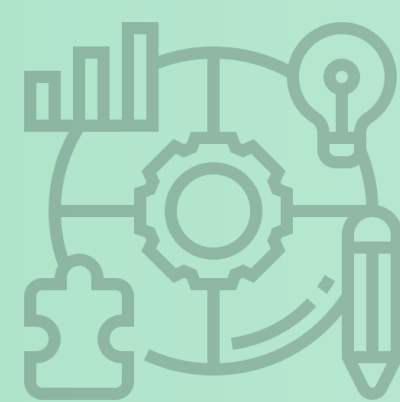
## What we want to understand:

The **applicability** of the UK Computer Misuse Act 1990 to cases of technology-facilitated domestic abuse/IPV

Conduct a **systematic legal analysis** of court cases drawing on **legal databases**.

## Method

- **Legal System:** “Higher” Courts
- **Legal Databases:**
  - Westlaw: Commercial – Paywall
  - LexisNexis: Commercial – Paywall
  - British and Irish Legal Information Institute (Bailii): Charity – Open
- **Inclusion Criteria:** Courts of England & Wales
- **Search Term:** “Domestic Violence and Abuse”
- **Reviewed Documents:** Case Digests, Judgments and Law Reports.
- **Evaluation Template:** Trends over time in Spreadsheets
- **Coding Manual:** Yes/Unknown/Maybe/N/A/CoI



## Findings

- Identified over **500 cases** from three legal databases (January 2019 - May 2021)
- Tech abuse continues to be **prevalent and common** within the domestic abuse court cases we are analysing including via:
  - Phone (such as abusive text messages, phone calls, monitoring messages and contacts), Social media, Recording devices, CCTV in the home, and Threats to release private sexual images
- The CMA 1990 **could have been applied** to various cases:
  - Unauthorised access to their partner’s messages and social media accounts, and
  - Manipulated partner’s social media account, including deleting ‘Facebook friends’ and impersonating other men.



## Implications

- **Tech Abuse Definition:** Based on abuse patterns, we identified new nuances to tech abuse
- **Database:** We created an open-access database
  - Case name, Court, Representation, Judge, Judgement date, Decision/sentence, Case overview/relevant legislation, Tech abuse, Further domestic abuse details, Database found in
- **Disregard:** Expose the ongoing discounting of tech abuse as “real” abuse (versus physical abuse)
- **Escalation Trajectories:** Demographic details of perpetrators/victims
- **ML/NLP Challenge:** Future automation based on the coded dataset we provide

