Papers from the British Criminology Society Conference 2025

An Online Journal by the British Society of Criminology

Lost in Definition: Conceptual and Practical Challenges in Policing Cyberstalking

Authors:

Tahreem Tahir[1], PhD Student, University of Lancashire

Kelly Bracewell[2], Senior Research Fellow, University of Lancashire

Joanne Westwood[3], Professor of Social Work Education, University of Lancashire

Charlottle Barlow[4], Associate Professor in Criminology and Criminal Justice, University of Leeds

Word Count: 5990

Corresponding Author Email: ttahir3@lancashire.ac.uk

Institutional Address:

University of Lancashire,

School of Health, Social Work and Sport

Preston, PR1 2HE

Lost in Definition: Conceptual and Practical Challenges in Policing Cyberstalking

Tahreem TAHIR[1], Kelly BRACEWELL[2], Joanne WESTWOOD[3], Charlotte BARLOW[4]

Abstract

Cyberstalking is a growing concern within society, yet remains conceptually contested and inconsistently defined across law, research and practice. Cyberstalking can be understood as a pattern of unwanted, fixated and obsessive use of digital technologies to monitor, contact or pursue individuals. Internationally, legal frameworks have struggled to keep pace with such behaviours. Pre-digital UK stalking legislation often fails to protect victims of cyberstalking, leading to gaps in investigations and prosecution, particularly where anonymity and cross-jurisdiction issues arise.

This paper examines the definitional and practical challenges arising from ambiguity in how harassment, stalking and cyberstalking are distinguished across arenas. Legal uncertainty, inconsistent policy frameworks, and discretionary policing practices contribute to fragmented responses, underreporting and missed opportunities for victim protection. Reviewing legal, academic and clinical perspectives, the paper explores how definitional debates directly influence policing responses. Engaging with these debates is vital to improving cyberstalking case recognition, strengthening victim protection, and developing coherent policing strategies. It concludes by highlighting the need for research grounded in the lived experiences of victim survivors and frontline police practice.

Key words: stalking, legislation, cyberstalking, digital abuse, policing

[1] ttahir3@lancashire.ac.uk PhD Student, University of Lancashire
[2] KBracewell1@lancashire.ac.uk Senior Research Fellow, University of Lancashire
[3] JLWestwood2@lancashire.ac.uk Professor of Social Work Education, University of Lancashire
[4] C.Barlow@leeds.ac.uk Associate Professor in Criminology and Criminal Justice, University of Leeds

Introduction

Cyberstalking is a growing concern in the digital age, exposing major gaps in the criminal justice system (College of Policing, 2024). With internet use reaching 99% among UK adults aged 16-44 years (Office for National Statistics 2020), digital communication is embedded in everyday life and significantly shapes social interaction. While digital technologies bring communication and connectivity, opportunities for abuse have also multiplied and exposed the conceptual and legislative limitations underpinning inconsistent policing of cyberstalking (Dragiewicz et al., 2018).

A central challenge in responding to cyberstalking lies in how police recognise, classify and respond to these behaviours. Research suggests officers frequently misclassify or minimise both 'traditional' stalking and cyberstalking, particularly in digital contexts (Taylor-Dunn & Erol, 2022). This affects recording, risk assessment and early safeguarding. This issue forms the central theme of this paper: lack of definitional clarity surrounding cyberstalking creates significant practical difficulties for policing.

Stalking is understood as a pattern of behaviour directed at an individual, involving repeated (two or more occasions) instances of unwanted visual and physical proximity, non-consensual communication, or threatening acts that instil fear in the victim (Wilson et al., 2022). While stalking has traditionally involved physical proximity, the increased use of digital technologies has facilitated the rise in cyberstalking whereby perpetrators exploit the internet and electronic communications to pursue their victim (Marcum et al., 2017).

There are no clear or agreed definition or criteria for cyberstalking (Nobles et al., 2014; Wilson et al., 2022). Rather than a single, unified definition, the literature presents a broad spectrum of behaviours that could be classified as cyberstalking. These behaviours typically include repetitive, persistent and unwanted communication or contact targeting an individual through electronic methods, including the internet and social media (Marcum et al., 2017; Nobles et al., 2014; Strawhun et al., 2013) to

intimidate, threaten and harm victims. Examples include a range of perpetrator behaviours, enabled through sophisticated use of technologies, relentless phone contact (Freed et al., 2018), doxing (exposing private information without consent) (Macallister, 2017), professional and personal sabotage (Tokunaga & Aune, 2017), spoofing (impersonating by falsifying information to deceive) (Horsman & Conniss, 2015), revenge porn (Finkelhor et al., 2023), swatting (fraudulent emergency call intended to incite a police response to victims location) (Mery & Mery, 2021), and using social media and surveillance applications for coercive control (Todd et al., 2021).

Measuring the prevalence of cyberstalking is challenging. Firstly, due to the rapid evolution and availability of digital technologies and its covert nature. Secondly, varied definitions across legal, academic, and clinical contexts result in inconsistent understanding, recording and response (The Suzy Lamplugh Trust, 2019) contributing to underrepresentation in statistics (Reyns & Fisher, 2018; Stonard, 2021; Strawhun et al., 2013).

For example, there are discrepancies in definition, sampling, and differing methodological approaches across studies (Kalaitzaki, 2019). Estimates suggest that cyberstalking impacts approximately 20 to 40 percent of online users worldwide (Reyns et al., 2012; Tokunaga & Aune, 2017). Technology-facilitated abuse, including cyberstalking, disproportionately affects women (Henry & Powell., 2018), reflecting the gendered nature of technology-facilitated abuse and interpersonal violence more broadly (Enock et al., 2024). These disparities undermine prevalence rates and the ability to safeguard victims.

The Definitional Maze

Cyberstalking is linked with severe significant psychological, physiological and functional harm including, anxiety, depression, hypervigilance, fear, post-traumatic stress disorder, and insomnia (Kaur et al., 2021). These harms are intensified by the persistent and often inescapable nature of digital abuse, which erodes victims' sense of

safety and stability (Kaur et al., 2021). However, police and prosecutors continue to struggle with identifying patterns, gathering evidence and applying existing offences highlighting the need to examine the statutory framework shaping current responses.

Statutory Framework

There is no standalone offence for 'cyberstalking' in England and Wales. Instead, cases are prosecuted under the *Protection from Harassment Act (1997) (PHA)*, including *s2* (Harassment), *s2A* (Stalking), *s4* (putting people in fear of violence), and *s4A* (Stalking involving fear of violence or serious alarm or distress). The Crown Prosecution Service, (2023a) also notes s42A (1) of the (Criminal Justice and Police Act, 2001), covering harassment of a person in their home, and racially or religiously aggravated forms of harassment under *s32* of the *Crime and Disorder Act (1998)*.

However, there is a lack of clarity surrounding the statutory definitions of 'stalking' and 'harassment' (HMIC & HMCPSI, 2017). Existing legislations for 'traditional' stalking is criticised as difficult for officers to interpret, with overlapping elements that create confusion between stalking and harassment (HMIC & HMCPSI, 2017). This leads to missed patterns, inconsistent identification of stalking offences, and cases being charged under wrong legislation. It is, therefore, unsurprising that there is further ambiguity in digital contexts.

The Ambiguity of Harassment

The offence of stalking was introduced by the *Protection from Harassment Act (1997)* to address repeated conduct causing alarm or distress in contexts such as a neighbour dispute, workplace bullying and similar persistent behaviours (Crown Prosecution Service, 2023a). Given that most victims are stalked by their partners or ex-partners it could be argued that legislation has always been ill-suited to tackle the complex dynamics of stalking. This misalignment is evident in section one of the act which broadly prohibits harassment without defining stalking and adds ambiguity that has complicated enforcement from the outset (Bliss, 2019).

Under s1(1) the defendant must not pursue a '*course of conduct'* which (a) amounts to harassment and (b) which they know or ought to know amounts to harassment. The '*ought to know'* is objective and amounts to harassment if a 'reasonable person' with the same information would think the conduct amounted to harassment (s1(2)). A '*course of conduct'* is defined as occurring at least two occasions (s7(3)) and causing *alarm or distress* to the victim (s7(2)).

This '*course of conduct'* requirement creates evidential barriers in cases that do not present a clear pattern and where incidents occur in isolation (Diaz, 2022). Victims often experience escalating behaviours however, this perception rarely aligns with the legal threshold (Scott, 2020). As a result, for isolated incidents, officers must rely on alternative offences or protective measure while waiting for a pattern to emerge (Crown Prosecution Service, 2023a). This delay exposes the victim to further risk and highlights how the legal framework fails to provide timely protection (HMICFRS, 2024). This creates evidential challenges and inconsistent thresholds for prosecution (Bliss, 2019).

Two aspects contribute to confusion. First, harassment is not defined in the Act beyond reference to '*alarm or distress'*, leaving the distinction between uncomfortable behaviour and a criminal pattern to the judgement of victims and individual police officers. For example, a small number of unwanted contacts is relatively common at the start or end of a relationship (e.g., De Smet et al., 2015) which makes relying solely on repetition to define harassment and stalking questionable. Second, the requirement of conduct on '*at least two occasions'* means that a single serious incident cannot qualify, while incidents that are dispersed or varied may not be recognised as part of one '*course of conduct'* unless linked during early police investigation. Where early reports are recorded as offences, such as public order, malicious communications, threats to kill or others, later escalation becomes more difficult to reframe into a pattern of harassment or stalking. Consequently, reviews such as HMIC & HMCPSI (2017) found victims held a profound lack of confidence in the criminal justice system and recommended a separate offence of stalking.

The Evolution of Stalking

Stalking was introduced by the *Protection of Freedom Act (2012*), which inserted s2A and s4A into the *Protection from Harassment Act (1997)*. It retains the harassment framework (*course of conduct*; *knows/ought to know*; *alarm/distress*) and adds a non-exhaustive list in s2A (3) of behaviours including *following, contacting, publishing material, monitoring online use, loitering, inferring with property, and surveillance* (Crown Prosecution Service, 2023). Stalking is a complex crime that may not involve direct violence but rather the threat of violence (Logan & Walker, 2017). As with harassment, there is no statutory definition of '*stalking*', leaving the boundary between harassment (*s2*) and stalking (*s2A*) unclear.

For the aggravated offence s4A of the Protection from Harassment Act (1997), the prosecution must prove stalking plus one of the two additional elements:

(i) Repeated fear or violence (the victim fears, on at least two occasions that violence will be used), or
(ii) Serious alarm or distress causing a substantial adverse effect on day-to-day activity.

The evidential threshold makes the offence dependent on proving fear, whether of *repeated violence* or of serious *alarm and distress*. The fear factor mandates that the victim feel specific emotions and fear to constitute the crime (Reyns & Englebrecht, 2013) rather than reliance on the perpetrators conduct. Yet, how fear should be defined and measured is debated (Wilcox, 1998). Fear can be conceptualised subjectively: involving emotional responses triggered by cognitive processes; feeling scared, afraid, fearful or frightened. Or objectively: considering behaviours that would cause fear in a reasonable person (Garofalo, 1981; Wilcox, 1998). This distinction between subjective and objective fear is central to assessing victim harm and the seriousness with which the offence is prosecuted (Wilcox, 1998). However, research shows that stalking victims

often experience psychological, social and practical harms without necessarily reporting fear (Storey et al., 2023; Tjaden et al., 2000; Fissel et al., 2022). This gap means some victims fall outside the legal definition, exposing fundamental flaws in existing thresholds that rely on demonstrating fear rather than recognising patterns of behaviour. Indeed, reports by HMIC & HMCPSI (2017) and HMICFRS (2024) reveal persistent confusion in applying stalking offences, with frequent mischarging between sections 2A and 4A. This undermines consistency in charging and case outcomes. In contrast, In Scotland, stalking is addressed as a standalone offence under s.39 of (*The Criminal Justice and Licensing (Scotland) Act*, 2010) which avoids combining stalking and harassment and makes it easier for officers and prosecutors to recognise (Middlemiss, 2014).

In sum, existing legislation in England and Wales remains reactive and narrow, failing to reflect the complex dynamics of stalking. This has further implications for digital contexts.

Problems in Defining Cyberstalking

Where harassment is defined only in broad statutory terms, stalking is reduced to illustrative behaviours, and cyberstalking remains unrecognised in law, the phenomenon becomes 'lost in definition'. Introduced before widespread internet use, existing legislation was never designed to address digital harassment or stalking (Stephen, 2017). Although terms such as '*course of conduct'*, '*contact'*, '*monitoring*', appear within the legislation, as detailed above, none make explicit reference to digital methods (HMIC & HMCPSI, 2017).

The Protection from Harassment Act (1997) and its amendments were never designed to encompass technology-facilitated abuse. Consequently, police and courts rely on analogies with offline behaviour. This has resulted in misclassification, inconsistent policing, and diminished victim confidence (Bliss, 2019) and is evident in the underreporting and under recording of stalking and cyberstalking (HMIC & HMCPSI, 2017). Evidence from HMICFRS and HMCPSI's *Living in Fear (2017)* reveals that online behaviours were overlooked, with patterns of conduct across multiple platforms often

missed. These problems are compounded by statutory overlap, which distorts the boundaries between harassment, stalking and cyberstalking.

In terms of legislation, there is further academic disagreement around *repetition* and *course of conduct*. Mirroring traditional 'stalking' some studies classify a single severe act (e.g., a credible online death threat) as cyberstalking, while others require a pattern over time or focus more broadly on distress (Wilson et al., 2022). These definitional inconsistencies influence how prevalence is *measured,* contributing to wide variation across studies. The '*fear standard'* is also widely debated with regards to cyberstalking. A large-scale US survey showed that most cyberstalking victims did not report fear but reported distress, frustration and anger (Fissel et al., 2022). Insisting on fear ignores important dimensions of harm, creating tension between legal definitions and lived experiences.

Victims describe tactics such as perpetrators using fake social media profiles, persistent re-contact after blocking, use of spyware, GPS tracking, doxing, repeated online contact, harassment, unwanted sexual advances, online threats of violence, and identity fraud (HMIC and HMCPSI, 2017; Crown Prosecution Service, 2023a), yet these behaviours are absent from the examples detailed in existing legislation. This leaves police and prosecutors reliant on broad terms such as '*contact*' or '*monitoring'* to interpret online conduct, a process that varies in cases (Crown Prosecution Service, 2023a; HMIC & HMCPSI, 2017). The borderless and ubiquitous nature of the internet compounds the issues, as victims can be subjected to constant intrusion. Without explicit legal recognition, these behaviours are overlooked or treated as minor (Bliss, 2019). In practice, the law makes it easier for police to overlook cyberstalking, with police often categorising incidents under alternative offences, obscuring its true prevalence (HMIC & HMCPSI, 2017).

Reliance on alternative legislation distorts official statistics and contributes to misconceptions of the issue. Depending on the circumstances, cyberstalking incidents can be placed under the *Malicious Communications Act* (1988), the *Communications Act* (2003) or the *Computer Misuse Act* (1990). These laws focus on technology, but do

not capture the pattern of behaviour that characterises stalking. The *Online Safety Act (2023)* aims to regulate harmful online activity by requiring social media platforms to remove illegal harmful content and safeguard users. It is enforced by the Office of Communications (OFCOM) rather than the police (Online Safety Act, 2025) and introduces no new criminal offences. Instead, it introduces a regulatory layer rather than a substantive criminal justice response. This leaves victims of cyberstalking reliant on pre-existing legislation, such as the *Protection from Harassment Act (1997)*, a law never designed for the digital age, as detailed earlier.

International Contrast

Other jurisdictions have attempted to address challenges posed by cyberstalking. In Canada, harassment and stalking are addressed under *s.264* of the *Criminal Code (1985)* which includes electronic communications such as email, social media and other digital intrusions. However, legislation struggles to keep pace with rapidly evolving digital behaviours, producing inconsistent police responses and evidential difficulties (Wang et al, 2025). Similar to England and Wales, Canadian statutory frameworks also lack clear distinction between harassment and stalking.

In Germany (S238 of the German Criminal Code (StGB) and Italy's 'atti persecutori' (persecutor acts) criminalises 'unwanted pursuit behaviours' without requiring physical proximity, enabling digital behaviours to be interpreted as stalking. These frameworks reduce statutory ambiguity, but challenges remain when *fear* and *distress* are used as the threshold.

In Australia, stalking laws in Queensland and Victoria explicitly include online contact, social media messages, GPS tracking and impersonation as stalking behaviours under *the Criminal Law Consolidation Act (1935)* (SA) s.19AA. In the United States, many states have specific cyberstalking laws. For example, Florida defines it as 'repeated electronic communication causing substantial emotional distress' serving no legitimate purpose. These provisions offer clear guidance for identifying digital abuse, reducing uncertainty for victims and police. However, varying thresholds across states create legal uncertainty

and inconsistent protection. This brief comparison is illustrative rather than comprehensive, given the complexity of multi-jurisdictional framework. It does, however, raise the question as to whether the UK should introduce a precise, technology-specific definition to reduce reliance on broad harassment legislation and improve recognition.

Cyberstalking: Academic and Clinical Literature

Academic Definitions

Criminological and Sociological research has examined stalking through behavioural patterns and conceptual boundaries (Bocij & Mcfarlane, 2002; Sheridan & Grant, 2007). Early work, such as Meloy's (1998) historically important but now outdated contribution, framed cyberstalking as *"a paranoid tinged world of malicious and intrusive activity on the internet"* while Spitzberg & Hoobler, (2002) described it as '*persistent and unwanted contact via technology'* emphasising repeated intrusion over specific acts. Wilson et al's (2022) research found substantial conceptual variations in definitions: some require repeated behaviour, others accept a single incident; some prioritise fear, others general distress; and views differ on whether indirect tactics like impersonation or surveillance count. These disparities complicate how prevalence is measured and hinder policy developments and policing responses.

Academic debates on cyberstalking reveal significant differences and overlaps. Early work positioned cyberstalking as an extension of traditional stalking; that when stalking moves online, the behaviours become more intrusive due to technology allowing constant access, increased monitoring and the ability to cross personal boundaries (Meloy, 1998). Others later argued that cyberstalking mirrors offline stalking involving similar motives, patterns of behaviour, control and relationships (Cavezza & McEwan, 2014; Sheridan & Grant, 2007). From these perspectives, technology changes the *method* of stalking, not its *nature*. More recently, emphasise has focused on the distinct characteristics of cyberstalking, such as anonymity, persistence, impersonations, constant access, covert surveillance and wide reach that sets it apart from traditional

stalking (Kaur et al., 2021, Kim, 2023). Some of these behaviours mirror coercive control in intimate or family relationships, however, cyberstalking also occurs outside those contexts, meaning it cannot be assumed to be inherently synonymous with coercive control (Dragiewicz et al., 2018). Nobles et al (2014) argue that cyberstalking victims endure longer victimisation, adopt self-protective behaviours (changing routine, avoiding social contact, quitting jobs) and face higher financial costs. Perpetrators often conceal their identity through fake profiles or untraceable accounts and victims report severe emotional consequences (Worsley et al., 2017). These factors require cyberstalking to be treated as a unique form of abuse, not subsumed under existing problematic definitions.

Further complexity lies in terminology of behaviours. Researchers use terms such as cyber-harassment, cyberbullying, and cyberstalking interchangeably, which blurs distinctions further. For instance, cyberbullying research includes impersonation, exclusion, threats and stalking (Łosiak-Pilch et al., 2022). Bussu et al. (2025) found that incidents in higher education labelled as cyberbullying often aligned more closely with cyberstalking. When cyberstalking is treated as harassment or bullying, it risks downplaying its seriousness. Again, this lack of clear terminology adds a further layer of definitional drift which hinders legal and policy responses.

These issues reinforces a need to incorporate more survivor-centred definitions that reflect lived impact rather than relying solely on narrow legal categories.

Clinical Definitions

Clinical literature on stalking has explored motivational typologies, including the rejected, intimacy-seeker, incompetent suitor, resentful, and predatory stalker (Mullen et al., 1999). However, their relevance is questioned due to their clinical focus and limited practical use. Their application to cyberstalking is also inadequate. Weekes et al (2025) question whether the existing typologies sufficiently categorise cyberstalking perpetrators arguing that they typically lack social skills, have low self-control and use digital surveillance tactics that do not easily align with traditional typologies. (Sheridan &

Grant, 2007) questioned whether cyberstalking its within existing stalking typologies or represents distinct motivations and behavioural pattern. Despite this early challenge, clinical stalking theory still remains underpeopled (Parkhill et al., 2022). Although different psychological theories such as attachment and social learning theory have been applied, none sufficiently guide diagnosis or intervention.

Psychiatry and psychology, typically define stalking by *impact* and *repetitive intrusiveness* (Mullen et al., 1999; Prabhu et al., 2019) rather than by a fixed behavioural checklist. Clinical perspectives focus on consequences such as trauma, sleep disturbances, and impaired functioning (Prabhu et al., 2019). Neither the DSM-5 nor ICD-11 (manuals to diagnose mental health conditions) recognise stalking or cyberstalking as diagnostic categories, leaving clinicians without guidance for assessing such harms. Furthermore, existing risk assessment tools do not capture online behaviours (Gamache et al., 2022). Although newer cyberstalking scales have developed, making comparisons across studies is difficult (Wilson et al (2022). The lack of standardisation leaves clinicians and police without reliable tools for identifying risk, reinforcing inconsistent recognition and recording and inadequate victim protection.

Victims often report psychological harm such as anxiety, hypervigilance, and social withdrawal due to cyberstalking (Fissel, 2021; Short et al., 2015), however, they may not necessarily identify fear, as noted earlier. From the clinical perspective, these harms are sufficient to gain recognition of cyberstalking. This contrasts with legal and operational policing perspectives which undermines consistent protection, discussed above. Without alignment, victims may receive therapeutic support but remain vulnerable to inadequate legal remedies and operational responses.

Practical Policing Challenges

Recognition and Recording: From '*incident*' to '*course of conduct*'

As discussed, cyberstalking is often treated by frontline officers as a series of unrelated incidents rather than a '*course of conduct*' (HMIC & HMCPSI, 2017). The difficulty of recognising patterns from disconnected reports is not unique to policing stalking; similar problems appear in police responses to coercive control (Walklate & Fitz-Gibbon, 2019). When cases are handled incident by incident, victims are repeatedly required to retell their experiences to different officers, which fragments their narrative and undermines confidence in police responses.

Cyberstalking is often minimised by police, treated as isolated incidents, and met with poor responses - leaving victims feeling 'invisible' (Korkodeilou, 2014; Taylor-Dunn & Erol, 2022). Such concerns were raised in the national stalking super-complaint, where victims reported that persistent online behaviour is not taken seriously or recognised as stalking even where there is a clear pattern of behaviour (HMICFRS, 2024). While some of these failures are attributable to individual policing practices, they reflect the deeper structural consequence: without precise stalking and cyberstalking definitions frontline policing faces uncertainty in decision-making.

Identification of Cyberstalking

Police lack confidence in responding to cyberstalking. For example, a study which found officers who report confidence identifying stalking often lack confidence when behaviours occur online. Williams et al (2021) found that while 96% of officers surveyed across two British police forces felt confident distinguishing stalking from harassment, fewer reported confidence doing so in cyberstalking cases (61%). Further, almost 38% expressed low confidence in recognising cyberstalking behaviours. This raise concerns around subsequent minimisation or misclassification and poor response and ultimately leads to distorted recording and prevalence data (HMIC & HMCPSI, 2017). These challenges are exacerbated by the speed at which digital technologies and behaviours evolve.

The absence of a screening tool for cyberstalking compounds the problem. The national stalking super-complaint highlighted victims felt pressured to *prove* the seriousness of digital incidents before they were recognised as victims, especially where the cyberstalking occurred through repeated friend requests, third-party messages or impersonation accounts (HMICFRS, 2024). This suggests that police responses may rely on individual discretion and may illustrate wider misunderstandings about the seriousness of cyberstalking. Given rapid technological change, any framework based on fixed categories risks quickly becoming outdated and unable to capture novel emerging behaviours. Nevertheless, a framework that provides a stable reference point for practitioners and policymakers is needed, even if it requires regular review and adaptive mechanisms to remain relevant.

Frontline officers often lack clarity on how to capture and present social media evidence or how to approach platforms for disclosure of online activity (Wall, 2013). More recently the HMICFRS (2024) super-complaint found breaches of stalking protection orders, supported by screenshots, yet significant delays in police action. The evidential challenge is compounded as police are under pressure to regulate social media - a 'privately owned but publicly populated' environment (Wall, 2013) - leaving them dependent on the cooperation of platforms whose priorities diverge from the criminal justice system. Without a clear accessible definition of cyberstalking or official guidance on evidential thresholds, officers lack the blueprint for what to collect, from where and with what degree of urgency. This conceptual uncertainty explains operational hesitation: evidential gaps, inconsistent case-building and delayed CPS decisions, ultimately undermining and impacting the victim (HMICFRS, 2024).

Officers' knowledge, Training and Discretion

Discretion is amplified where legal definitions are vague. Without cyberstalking specific statutory or policy guidance, officers rely on professional judgement rather than specific criteria, leading to variations in responses. Korkodeilou (2014) noted victims'

experiences often reflect misconceptions of stalking dynamics and over-reliance on their evidence. Taylor-Dunn & Erol (2022) found shortcomings in the use of police risk assessment tools when it comes to online abuse.

Police knowledge of what constitutes digital evidence is inconsistent. Korkodeilou (2014) found operational officers relied on personal discretion to determine what counts as digital evidence leading to variations and inconsistencies. Victims in the super-complaint described being passed between multiple officers, each unfamiliar with their cases, resulting in repeated re-telling of traumatic events and fragmented investigations (HMICFRS, 2024). Taylor-Dunn & Erol (2022) indicated that victims continue to report the same inadequate police responses, even after the *Protection of Freedom Act (2012),* introduced to close the gap between legislation and policing practice. The persistence of these failings highlights a deeper structural disconnect: officers are still expected to interpret digital behaviours through legislative and policing frameworks designed for traditional stalking, leaving core practices unchanged in how cyberstalking is recognised, recorded and assessed. Operational tools and procedures guiding officers have not been meaningfully updated to reflect the realities of cyberstalking. Without survivor-informed, adaptable tools that capture technological and contextual nuances, risk assessment will remain outdated and ineffective, failing to capture the true scope and severity of harm.

Conclusion

Cyberstalking remains ‘lost in definition’ within law, academia and policing. The mismatch between outdated legal frameworks and the fast-evolving nature of technology means cyberstalking as a phenomenon is consistently under-recognised and poorly risk assessed in practice. The core challenges lie in the absence of clear definitions, limitations in current legislation, and difficulties in identifying and assessing digital patterns of harm. These gaps leave victims exposed and unprotected while stalking and cyberstalking escalates. Without clear definitions and effective tools, cases are under-reported, misclassified and poorly managed. Reliance on outdated frameworks means

policies fail to address technological change and lived experiences, resulting in missed opportunities for early intervention and inadequate victim protection.

Drawing on experiences as a former police officer, the lead author has witnessed how definitional ambiguity and incident-focused practices weakens effective policing responses to stalking and cyberstalking, leaving victims at risk. Building on these experiences, Tahir's doctoral research examines police officers' response to young people's experiences of cyberstalking, with the aim to bridge the knowledge gap between academia and frontline practice. By linking these perspectives, this research aims to contribute to survivor-centred policing approaches that improves recognition, safeguarding and delivers effective responses for victims.

Reference

Bocij, P., & Mcfarlane, L. (2002). Online harassment: towards a definition of cyberstalking. *Prison Service Journal*, *139*, 31–38. www.harassment-law.co.uklbook!cyberep.htm.

Bussu, A., Pulina, M., Ashton, S. A., & Mangiarulo, M. (2025). Cyberbullying and cyberstalking in higher education: policies and practices for supporting students and university staff. *Social Psychology of Education*, *28*(1). https://doi.org/10.1007/s11218-024-09989-x

College of Policing. (2024). *Victim experience of the police response to stalking: Rapid evidence review to support the investigation into the super-complaint on the police response to stalking*.

Costa, D., Soares, J., Lindert, J., Hatzidimitriadou, E., Sundin, Ö., Toth, O., Ioannidi-Kapolo, E., & Barros, H. (2015). Intimate partner violence: a study in men and women from six European countries. *International Journal of Public Health*, *60*(4), 467–478. https://doi.org/10.1007/s00038-015-0663-1

Crime and Disorder Act. (1998). https://www.legislation.gov.uk/ukpga/1998/37/contents

Criminal Code. (1985). https://laws-lois.justice.gc.ca/eng/acts/C-46/section-264.html?txthl=harassment+harassed

Crown Prosecution Service. (2023a). *Stalking and harassment: Legal guidance*. https://www.cps.gov.uk/legal-guidance/stalking-and-harassment

Crown Prosecution Service. (2023b, April 24). *Stalking or Harassment*. https://www.cps.gov.uk/legal-guidance/stalking-or-harassment

De Smet, O., Uzieblo, K., Loeys, T., Buysse, A., & Onraedt, T. (2015). Unwanted Pursuit Behavior After Breakup: Occurrence, Risk Factors, and Gender Differences. *Journal of Family Violence*, *30*(6), 753–767. https://doi.org/10.1007/s10896-015-9687-9

Diaz, M. (2022). Exploring Multiple-Perpetrator Stalking: Victim Consequences of Solo and Multiple Stalkers. *Victims and Offenders*, *17*(1), 78–100. https://doi.org/10.1080/15564886.2021.1900004

Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N. P., Woodlock, D., & Harris, B. (2018). Technology facilitated coercive control: domestic violence and the competing roles of digital media platforms. *Feminist Media Studies*, *18*(4), 609–625. https://doi.org/10.1080/14680777.2018.1447341

Enock, F. E., Stevens, F., Bright, J., Cross, M., Johansson, P., Wajcman, J., & Margetts, H. Z. (2024). *Understanding gender differences in experiences and concerns surrounding online harms: A short report on a nationally representative survey of UK adults*. http://arxiv.org/abs/2402.00463

Finkelhor, D., Turner, H., & Colburn, D. (2023). Which dynamics make online child sexual abuse and cyberstalking more emotionally impactful: Perpetrator identity and images? *Child Abuse and Neglect*, *137*. https://doi.org/10.1016/j.chiabu.2023.106020

Fissel, E. R. (2021). The Reporting and Help-Seeking Behaviors of Cyberstalking Victims. *Journal of Interpersonal Violence*, *36*(11–12), 5075–5100. https://doi.org/10.1177/0886260518801942

Fissel, E. R., Reyns, B. W., Nobles, M. R., Fisher, B. S., & Fox, K. A. (2022). Cyberstalking Victims' Experiences With Fear Versus Other Emotional Responses to Repeated Online Pursuit: Revisiting the Fear Standard Among a National Sample of Young Adults. *Crime and Delinquency*. https://doi.org/10.1177/00111287221096374

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2018). "A stalker's paradise": How intimate partner abusers exploit technology. *Conference on Human Factors in Computing Systems - Proceedings*, *2018-April*. https://doi.org/10.1145/3173574.3174241

Gamache, D., Savard, C., Faucher, J., & Cloutier, M. È. (2022). Development and Validation of the Stalking and Obsessive Relational Intrusions Questionnaire (SORI-Q). *Journal of Interpersonal Violence*, *37*(21–22), NP19420–NP19446. https://doi.org/10.1177/08862605211042808

Garofalo, J. (1981). The Fear of Crime: Causes and Consequences. *The Journal of Criminal & Criminology*, *72*(2), 839–857. https://doi.org/0091-4169/81/7202-0839

Henry, N., & Powell, A. (2018). Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research. *Trauma, Violence, and Abuse*, *19*(2), 195–208. https://doi.org/10.1177/1524838016650189

HMIC, & HMCPSI. (2017). *Living in fear-the police and CPS response to harassment and stalking A joint inspection by HMIC and HMCPSI*. www.justiceinspectorates.gov.uk/

HMICFRS. (2024). *Police response to stalking. London: His Majesty's Inspectorate of Constabulary and Fire & Rescue Services*. https://hmicfrs.justiceinspectorates.gov.uk/publications/suzy-lamplugh-trusts-super-complaint-the-police-response-to-stalking/

Horsman, G., & Conniss, L. R. (2015). An investigation of anonymous and spoof SMS resources used for the purposes of cyberstalking. *Digital Investigation*, *13*, 80–93. https://doi.org/10.1016/j.diin.2015.04.001

Kalaitzaki, A. (2019). Cyberstalking victimization and perpetration among young adults: Prevalence and correlates. In *Recent Advances in Digital Media Impacts on Identity, Sexuality, and Relationships* (pp. 22–38). IGI Global. https://doi.org/10.4018/978-1-7998-1063-6.ch002

Kaur, P., Dhir, A., Tandon, A., Alzeiby, E. A., & Abohassan, A. A. (2021). A systematic literature review on cyberstalking. An analysis of past achievements and future promises. *Technological Forecasting and Social Change*, *163*. https://doi.org/10.1016/j.techfore.2020.120426

Kevin Wang, S. Y., Mei, X., Hsieh, M. L., Cao, L., & Li, Z. S. (2025). Cyber victimization and social cohesion: Unraveling correlates of cyberbullying and cyberstalking in Canada. *International Journal of Law, Crime and Justice*, *82*. https://doi.org/10.1016/j.ijlcj.2025.100766

Korkodeilou, J. (2014). Dealing with the unknown: Learning from stalking victims' experiences. *Crime Prevention and Community Safety*, *16*(4), 253–268. https://doi.org/10.1057/cpcs.2014.10

Logan, T. K., & Walker, R. (2017). Stalking: A Multidimensional Framework for Assessment and Safety Planning. *Trauma, Violence, and Abuse*, *18*(2), 200–222. https://doi.org/10.1177/1524838015603210

Łosiak-Pilch, J., Grygiel, P., Ostafińska-Molik, B., & Wysocka, E. (2022). Cyberbullying and its protective and risk factors among Polish adolescents. *Current Issues in Personality Psychology*, *10*(3), 190–204. https://doi.org/10.5114/cipp.2021.111404

Macallister, J. M. (2017). The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information. In *Fordham Law Review* (Vol. 85). https://ir.lawnet.fordham.edu/flr/vol85/iss5/44

Marcum, C. D., Higgins, G. E., & Nicholson, J. (2017a). I'm Watching You: Cyberstalking Behaviors of University Students in Romantic Relationships. *American Journal of Criminal Justice*, *42*(2), 373–388. https://doi.org/10.1007/s12103-016-9358-2

Marcum, C. D., Higgins, G. E., & Nicholson, J. (2017b). I'm Watching You: Cyberstalking Behaviors of University Students in Romantic Relationships. *American Journal of Criminal Justice*, *42*(2), 373–388. https://doi.org/10.1007/s12103-016-9358-2

Meloy, J. R. (1998). *The psychology of stalking: Clinical and forensic perspectives*. https://doi.org/https://doi.org/10.1016/B978-012490560-3/50020-7

Mery, H., & Mery, H. C. (2021). *The Dangers of Doxing and Swatting: Why Texas Should Criminalize These Malicious Forms of Cyberharassment* (Vol. 52). https://time.com/5189945/

Middlemiss, S. (2014). Let the Stalker Beware? Analysis of the Law of Stalking in Scotland. *Journal of Criminal Law*, *78*(5), 407–422. https://doi.org/10.1350/jcla.2014.78.5.942

Nobles, M. R., Reyns, B. W., Fox, K. A., & Fisher, B. S. (2014). Protection Against Pursuit: A Conceptual and Empirical Comparison of Cyberstalking and Stalking Victimization Among a National Sample. *Justice Quarterly*, *31*(6), 986–1014. https://doi.org/10.1080/07418825.2012.723030

Office for National Statistics. (2020). *Internet users, UK 2020*. https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2020

Online Safety Act. (2025). *Explains the Act's duties on platforms to safeguard users and remove illegal content*. https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer

Parkhill, A. J., Nixon, M., & McEwan, T. E. (2022). A critical analysis of stalking theory and implications for research and practice. *Behavioral Sciences and the Law*, *40*(5), 562–583. https://doi.org/10.1002/bsl.2598

Paullet, K., Rota, D., & Swan, T. (2009). Cyberstalking: an exploratory study of students at a Mid-Atlantic University. *Issues In Information Systems*. https://doi.org/10.48009/2_iis_2009_640-649

Prabhu, M., Pinals, D. A., Bayner, J., Benedek, E., Binder, R., Brandt, A., Champion, M., Datta, V., Ford, E., Frierson, R., Harding, L., Jain, A., Kraus, L., Park, B., Pruette, M., Thomas, T., & Zonana, H. (2019). *APA Resource Document Resource Document on Stalking, Intrusive Behaviors and Related Phenomena by Patients Prepared by the Council on Psychiatry and Law*.

Reyns, B. W., & Englebrecht, C. M. (2013). The Fear Factor: Exploring Predictors of Fear Among Stalking Victims Throughout the Stalking Encounter. *Crime and Delinquency*, *59*(5), 788–808. https://doi.org/10.1177/0011128712461123

Reyns, B. W., & Fisher, B. S. (2018). The relationship between offline and online stalking victimization: A gender-specific analysis. *Violence and Victims*, *33*(4), 769–786. https://doi.org/10.1891/0886-6708.VV-D-17-00121

Reyns, B. W., Henson, B., & Fisher, B. S. (2012). Stalking in the Twilight Zone: Extent of Cyberstalking Victimization and Offending Among College Students. *Deviant Behavior*, *33*(1), 1–25. https://doi.org/10.1080/01639625.2010.538364

Scott, A. J. (2020). *Stalking: How perceptions differ from reality and why these differences matter*.
Sheridan, L., & Grant, T. (2007). Is cyberstalking different? *Psychology, Crime and Law*, *13*(6), 627–640. https://doi.org/10.1080/10683160701340528
Short, E., Guppy, A., Hart, J. A., & Barnes, J. (2015). The Impact of Cyberstalking. *Studies in Media and Communication*, *3*(2), 23–37. https://doi.org/10.11114/smc.v3i2.970
Spitzberg, B. H., & Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. *New Media & Society*, *4*(1), 71–92. https://doi.org/https://doi.org/10.1177/14614440222226271
Stephen, A. (2017). Comparative Analysis of Cyber Stalking Legislations in UK, US and India. *Christ University Law Journal*, *6*(2), 61–76. https://doi.org/10.12728/culj.11.4
Stonard, K. E. (2021). The prevalence and overlap of technology-assisted and offline adolescent dating violence. *Current Psychology*, *40*(3), 1056–1070. https://doi.org/https://doi.org/10.1007/s12144-018-0023-4
Strawhun, J., Adams, N., & Huss, M. T. (2013). The assessment of cyberstalking: An expanded examination including social networking, attachment, jealousy, and anger in relation to violence and abuse. *Violence and Victims*, *28*(4), 715–730. https://doi.org/10.1891/0886-6708.11-00145
Taylor-Dunn, H., & Erol, R. (2022). Improving the 'victim journey' when reporting domestic abuse cyberstalking to the police – A pilot project evaluation. *Criminology and Criminal Justice*. https://doi.org/10.1177/17488958221129436
the Criminal Justice and Licensing (Scotland) Act. (2010). https://www.legislation.gov.uk/asp/2010/13/section/39
the Criminal Law Consolidation Act. (1935). https://www.legislation.sa.gov.au/search?query=stalking+
The Protection from Harassment Act . (1997). https://www.legislation.gov.uk/ukpga/1997/40/contents
The Suzy Lamplugh Trust. (2019). *What is stalking?* https://www.suzylamplugh.org/what-is-stalking
Todd, C., Bryce, J., & Franqueira, V. N. L. (2021). Technology, cyberstalking and domestic homicide: informing prevention and response strategies. *Policing and Society*, *31*(1), 82–99. https://doi.org/10.1080/10439463.2020.1758698
Tokunaga, R. S., & Aune, K. S. (2017). Cyber-Defense: A Taxonomy of Tactics for Managing Cyberstalking. *Journal of Interpersonal Violence*, *32*(10), 1451–1475. https://doi.org/10.1177/0886260515589564
Walklate, S., & Fitz-Gibbon, K. (2019). The criminalisation of coercive control: The power of law? *International Journal for Crime, Justice and Social Democracy*, *8*(4), 94–108. https://doi.org/10.5204/ijcjsd.v8i4.1205
Weekes, C. J., Storey, J. E., & Pina, A. (2025). Cyberstalking Perpetrators and Their Methods: A Systematic Literature Review. In *Trauma, Violence, and Abuse*. SAGE Publications Ltd. https://doi.org/10.1177/15248380251333411
Wilcox, R. P. (1998). A Re-examination of the crime fear linkage. *Journal of Research in Crime & Delinquency*.
Williams, M., Butler, M., Jurek-Loughrey, A., & Sezer, S. (2021). Offensive communications: exploring the challenges involved in policing social media. *Contemporary Social Science*, *16*(2), 227–240. https://doi.org/10.1080/21582041.2018.1563305

Wilson, C., Sheridan, L., & Garratt-Reed, D. (2022). What is Cyberstalking? A Review of Measurements. *Journal of Interpersonal Violence*, *37*(11–12), 1–28. https://doi.org/10.1177/0886260520985489

Worsley, J. D., Wheatcroft, J. M., Short, E., & Corcoran, R. (2017). Victims' Voices: Understanding the Emotional Impact of Cyberstalking and Individuals' Coping Responses. *SAGE Open*, *7*(2). https://doi.org/10.1177/2158244017710292