REPHRAIN

Protecting citizens online

# Towards a research agenda: Tackling violence against women and girls online.

Dr Ola Michalec, Dr Kim Barker, Dr Kovila Coopamootoo, Dr Lynne Coventry, Dr Francois Duppresoir, Dr Matthew Edwards, Prof Shane Johnson, Emily Johnstone, Prof Olga Jurasz, Dr Maryam Mehrnezhad, Prof Wendy Moncur, Frances Ridout, Francesca Stevens, Dr Angelika Strothmayer and Dr Leonie Tanczer.

UK Research and Innovation · University of Bristol · UCL · The University of Edinburgh · King's College London · University of Bath

April 2023

# Towards a research agenda: tackling violence against women and girls online


***REPHRAIN National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online***

***REPHRAIN White Paper, April 2023***

## 1. Introduction

Digital technologies have the capacity to bring about both societal benefits and harms. From established devices like smartphones, to innovations such as smart home speakers or health trackers, collectively, they require a renewed debate on safety, security, privacy and agency online.

It is important to highlight that harms and benefits of technologies are not distributed equitably in society. The UN estimates that globally one in three women and girls have been subjected to physical or sexual violence at least once in their lives. According to End Violence Against Women, women are 27 times more likely than men to be harassed online. Further, access to safety measures and advice is also gendered, with default designs and self-defence techniques failing to adequately address threats women and girls are typically subjected to (e.g., stalking, sexual harassment, control over reproductive cycles).

The topic is timely, with strategies set out by the national law enforcement agencies and policy bodies in the UK. For example, the National Police Chiefs' Council published the national Delivery Framework 'Policing violence against women and girls' in 2021 and the Home Office published a strategic document entitled 'Tackling Violence Against Women and Girls' in 2021. More recently, in November 2022, the government has announced new offences to tackle image-based sexual abuse (such as revenge porn or deepfakes), strengthening protections for victims. Although the change has been welcomed by experts in the area, there is plenty of scope for improvement, especially in the wake of the upcoming Online Safety Bill.

Following the publication of strategic documents and implementation plans, the next step is to review the current evidence, identify knowledge gaps, communicate recommendations and pose a set of outstanding challenges. Our report commences that process, with an outline of current research themes, a list of relevant publications, key research questions and a set of actionable recommendations to policymakers, law enforcement agencies and other practitioners.

This report is written by a group of researchers based at REPHRAIN, the National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online. REPHRAIN is the UK's world-leading interdisciplinary community focused on the protection of citizens online. As a UKRI-funded National Research Centre, 130 internationally leading experts at 17 UK institutions working across

46 different and diverse research projects and 23 founding industry, non-profit, government, law, regulation, and international research centre partners. As an interdisciplinary and engaged research group, we work collaboratively on addressing the three following missions:

· Delivering privacy at scale while mitigating its misuse to inflict harms;

· Minimising harms while maximising benefits from a sharing-driven digital economy;

· Balancing individual agency vs. social good.

Addressing violence against women and girls (VAWG) online is a key area of research focus of our centre. Collectively, we gather subject matter experts across psychology, criminology, political science, computer science, usable security, human-computer interactions and science and technology studies. As engaged and policy-oriented researchers, we work closely with users and practitioners to deliver outputs that adequately address the contemporary challenges of gendered violence in the context of digital technologies.

The aim of this document is to inform the emerging research agenda in the field.

The target audience of this report are: policymakers (e.g., Ofcom, Department for Digital, Culture, Media and Sport), law enforcement agencies (e.g., the National Crime Agency, Metropolitan Police) funding bodies (e.g., UK Research and Innovation, British Academy, Wellcome Trust) and, finally, developers of digital technologies (smart home devices, smartphones, FemTech etc.).

This report was edited by Dr Ola Michalec, Policy Engagement Associate at the REPHRAIN Centre. We would like to acknowledge the contribution of our subject matter experts (in alphabetical order): Dr Kim Barker, Dr Kovila Coopamootoo, Dr Lynne Coventry, Dr Francois Duppresoir, Dr Matthew Edwards, Prof Shane Johnson, Emily Johnstone, Prof Olga Jurasz, Dr Maryam Mehrnezhad, Prof Wendy Moncur, Frances Ridout, Francesca Stevens, Dr Angelika Strothmayer, and Dr Leonie Tanczer.

Please cite this report as: Michalec, O., Barker, K., Coopamootoo, K., Coventry, L., Duppresoir, F., Edwards, M., Johnson, S., Johnstone, Jurasz, O., E., Mehrnezhad, M., Moncur, W., Ridout, F., Stevens, F., Strothmayer, A., Tanczer, L. (2023) Towards a research agenda: tackling violence against women and girls online. REPHRAIN White Paper

## 2. Recent research topics

The REPHRAIN Centre has mobilised expertise in the following areas related to violence against women and girls:

- Domestic violence, intimate partner violence and their crossover into online spaces – e.g. via tech abuse, see project A4PL (Wendy Moncur)
- Gender gap in cybersecurity and privacy science and practices, e.g., confidence in protection from stalking and online tracking, see project AGENCY (Maryam Mehrnezhad)
- Complex harms and user agency in female-oriented technologies, e.g., fertility and period trackers, I.e., risks to reproductive rights in case of data breach or state surveillance (Maryam Mehrnezhad)

- Gender gap in access to privacy and security advice, online safety technologies and safety outcomes (Kovila Coopamootoo)
- Revictimisation, reporting and reactive challenges and trust issues in online advice such as from the police, see project AGENCY (Kovila Coopamootoo)
- Agency within smart homes and in relation to online harms such as harassment, misinformation (Kovila Coopamootoo)
- Psychology of perpetrators, their characteristics and justifications for using digital technology as a tool of abuse, see the EPSRC Centre for Doctoral Training in Cybersecurity at scale (PhD student Emily Johnstone).
- Current regulatory landscape at the intersection of online safety and Intimate Partner Violence, see project CMA1990 (Leonie Tanczer, Shane Johnson, Francesca Stevens, Frances Ridout)
- Protecting Girls from Online Harms in inner cities (Kim Barker, Olga Jurasz)
- The intersections between gender and IoT, see Gender and Tech group at UCL (led by Leonie Tanczer)
- Exploring interdisciplinary and intersectional perspectives in examining the global problem of online forms of violence against women, see the Observatory on Online Violence Against Women (led by Kim Barker and Olga Jurasz)

## 3. Recommended literature by the REPHRAIN researchers

REPHRAIN researchers boast a track record of high-quality scientific publications on gender and online harms. Below we offer a list of outputs published in peer-reviewed venues. We are happy to present these findings as policy roundtables or briefings upon request. Please contact us at rephrain-centre@bristol.ac.uk to explore your preferred methods of communication.

**Defining and measuring online harms**


- Almeida, T., Shipp, L., Mehrnezhad, M., & Toreini, E. (2022). Bodies Like Yours: Enquiring Data Privacy in FemTech. *Adjunct Proceedings of the 2022 Nordic Human-Computer Interaction Conference* (pp. 1-5). https://www.researchgate.net/publication/361925277_Bodies_Like_Yours_Enquiring_Data_Privacy_in_FemTech
- Coopamootoo, K. P., Mehrnezhad, M., & Toreini, E. (2022). "I feel invaded, annoyed, anxious and I may protect myself": Individuals' Feelings about Online Tracking and their Protective Behaviour across Gender and Country. *31st USENIX Security Symposium* https://www.usenix.org/system/files/sec22summer_coopamootoo.pdf
- Edwards, M., de Tangil Rotaeche, G. N. S., Peersman, C., Stringhini, G., Rashid, A., & Whitty, M. (2018). The geography of online dating fraud. *Workshop on technology and consumer protection (ConPro).* https://research-information.bris.ac.uk/ws/portalfiles/portal/152062431/geoscammy.pdf

**Understanding perpetrators**


- Grimani, A., Gavine, A., & Moncur, W. (2022). An Evidence Synthesis of Covert Online Strategies Regarding Intimate Partner Violence. *Trauma, Violence, & Abuse*, *23*(2), 581–593. http://wrap.warwick.ac.uk/147359/
- Lopez-Neira, I., Patel, T., Parkin, S., Danezis, G., & Tanczer, L. (2019). 'Internet of Things': How abuse is getting smarter. Safe – The Domestic Abuse Quarterly, (63), 22-26 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3350615
- Tanczer, L. M., López-Neira, I., & Parkin, S. (2021). 'I feel like we're really behind the game': perspectives of the United Kingdom's intimate partner violence support sector on the rise of technology-facilitated abuse. *Journal of gender-based violence*, 5(3), 431-450. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3931045


**Developing public services, policies and standards**


- Bellini, R., Strohmayer, A., Olivier, P., & Crivellaro, C. (2019). Mapping the margins: Navigating the ecologies of domestic violence service provision. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-13). https://core.ac.uk/download/pdf/327367258.pdf
- Branley-Bell, D., Coventry, L., Dixon, M., Joinson, A., & Briggs, P. (2022). Exploring Age and Gender Differences in ICT Cybersecurity Behaviour. *Human Behavior and Emerging Technologies*. https://rke.abertay.ac.uk/en/publications/exploring-age-and-gender-differences-in-ict-cybersecurity-behavio
- Chowdhury, P.D., Sameen, M., Blessing, J., Boucher, N., Gardiner, J., Burrows, T., Anderson, R. and Rashid, A., (2023) Threat Models over Space and Time: A Case Study of E2EE Messaging Applications. arXiv preprint https://arxiv.org/abs/2301.05653
- Stevens, F., Tanczer, L. M., Ridout, F., & Johnson, S. D. (2021). The Applicability of the UK Computer Misuse Act 1990 onto Cases of Technology-Facilitated Domestic Violence and Abuse. London: UK Home Office/University College London. https://www.ucl.ac.uk/computer-science/sites/computer_science/files/the_applicability_of_the_uk_computer_misuse_act_1990_onto_cases_of_technology_facilitated_domestic_violence_and_abuse.pdf
- Mehrnezhad, M., & Almeida, T. (2021). Caring for intimate data in fertility technologies. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1-11). https://www.researchgate.net/publication/349405322_Caring_for_Intimate_Data_in_Fertility_Technologies
- Mehrnezhad, M., Shipp, L., Almeida, T., & Toreini, E. (2022). Vision: Too Little too Late? Do the Risks of FemTech already Outweigh the Benefits? P*roceedings of the 2022 European Symposium on Usable Security* (pp. 145-150). https://eurousec2022.secuso.org/pre-proceedings/eurousec2022-final6.pdf

- Strohmayer, A., Laing, M., & Comber, R. (2017). Technologies and social justice outcomes in sex work charities: Fighting stigma, saving lives. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 3352-3364). https://core.ac.uk/reader/228158770


**Co-designing safer technologies**


- Parkin, S., Patel, T., Lopez-Neira, I., & Tanczer, L. (2019). Usability analysis of shared device ecosystem security: informing support for survivors of IoT-facilitated tech-abuse. *Proceedings of the new security paradigms workshop (pp. 1-15).* https://discovery.ucl.ac.uk/id/eprint/10083266/
- Coopamootoo, K. P. (2020). Usage patterns of privacy-enhancing technologies. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1371-1390). https://arxiv.org/abs/2009.10278
- Mehrnezhad, M., Coopamootoo, K., & Toreini, E. (2022). How Can and Would People Protect From Online Tracking? *Proceedings on Privacy Enhancing Technologies*, *1*, 105-125. https://petsymposium.org/popets/2022/popets-2022-0006.pdf
- Slupska, J., & Tanczer, L. M. (2021). Threat modeling intimate partner violence: tech abuse as a cybersecurity challenge in the Internet of Things. *The Emerald International Handbook of Technology-Facilitated Violence and Abuse.* Emerald Publishing Limited. https://discovery.ucl.ac.uk/id/eprint/10129049/
- Strohmayer, A., Slupska, J., Bellini, R., Coventry, L., Hairston, T., & Dodge, A. (2021). Trust and Abusability Toolkit: Centering Safety in Human-Data Interactions. https://nrl.northumbria.ac.uk/id/eprint/47508/1/TrustAndAbusabilityToolkit.pdf
- Strohmayer, A., Bellini, R., & Slupska, J. (2022). Safety as a Grand Challenge in Pervasive Computing: Using Feminist Epistemologies to Shift the Paradigm From Security to Safety. *IEEE Pervasive Computing*, 21(3), 61-69. https://www.rosiebellini.com/wp-content/uploads/2022/09/safety.pdf
- Suarez-Tangil, G., Edwards, M., Peersman, C., Stringhini, G., Rashid, A., & Whitty, M. (2019). Automatically dismantling online dating fraud. *IEEE Transactions on Information Forensics and Security*, 15, 1128-1137. https://core.ac.uk/download/pdf/224814353.pdf


**Improving the police practice and the justice system**


- Barker, K., & Jurasz, O. (2019). Online misogyny as hate crime: a challenge for legal regulation? (p. 146). Taylor & Francis. https://oro.open.ac.uk/57063/
- Barker, K., & Jurasz, O. (2021). Gender-Based Abuse Online: An Assessment of Law, Policy and Reform in England and Wales. The Palgrave Handbook of Gendered Violence and Technology, 529-544. https://oro.open.ac.uk/82190/
- Barker, K., & Jurasz, O. (2021). Text-Based (Sexual) Abuse and Online Violence Against Women: Toward Law Reform?. In The Emerald International Handbook of Technology-Facilitated Violence and Abuse (pp. 247-264). Emerald Publishing Limited.

https://www.emerald.com/insight/content/doi/10.1108/978-1-83982-848-520211017/full/html

## 4. What are the future research questions and priority areas?

Despite the recent research advances, there are numerous outstanding challenges with regards to tackling violence against women and girls online. This section contains specific problem areas and questions related to the themes such as: harms measurement, understanding perpetrators, developing policies and standards, co-designing safer technologies, and finally, improving the police practice and the criminal justice system. We hope that these research questions will inform strategic priorities of the relevant policy stakeholders and funding bodies.

**Defining and measuring online harms**

- **Consistency in measurement**: How to measure the extent of online harm types against women and girls and to quantify their impact?
- **Accurate reporting**: How do we ensure reporting mechanisms accurately capture intersectional experiences of harm? How do we ensure we are capturing the breadth of harms consistently in reporting mechanisms?
- **Gender gap**: How should we measure the gender gap with regards to access to security and privacy advice, and digital technologies?
- **Identification of emerging harms:** What is the range of harms associated with gender and modern technologies (e.g., FemTech, smart homes) and their impact on user agency? Are there any new harms that we currently do not capture?
- **Defining online harms**: How are online harms defined in law vs how they are experienced by women and girls (i.e., are lived experiences reflected and captured in law?)
- **Intersectionality:** How does this range of online harms differentially impact women and girls across demographics such as age, sexual orientation, gender identity, ethnicity, and socio-economic background? Are online harms experienced differently by girls compared to women?

**Understanding perpetrators**

- What are the perpetrator characteristics of those engaged in online harms against women and girls?
- How to explore researchers' positionality and language to enable rehabilitation of perpetrators?
- How and why do perpetrators exploit technology for abuse? How do they discuss and deploy strategies of technology abuse?
- How and why do perpetrators embed gender bias in their abuse?

- What are the technological affordances of devices and platforms for the perpetration of online harm against women and girls?

**Developing public services, policies and standards**

- How can the current and emerging regulations (e.g., GDPR, The Online Safety Bill, Data Protection and Digital Information Bill) address the cyber security and privacy gender gap?
- What are technical design recommendations, standards, best practices for including safety in the design of connected devices?
- How might safety recommendations be ethically designed and deployed without assigning blame to targets of abuse? How can these be designed to be inclusive of intersectional experiences of abuse?

**Co-designing safer technologies**

- How can we design safe, secure, and privacy-preserving systems to enable agency for victims and survivors? How to co-design such systems with multiple stakeholders such as the police and end users?
- How can we understand the safety needs of vulnerable user groups and co-design mechanisms to improve their agency with regards to safety from online harms?
- How to develop defence tools against stalkerware?

**Improving the police practice and the justice system**

- How can we redistribute responsibilities for violence prevention in a way which doesn't burden targets with the sole responsibility for their own safety? How can we draw on knowledge of perpetrator behaviours to train police/other members in the justice system to inform investigations and the journey to justice?
- What would trauma-informed training for judges and juries look like? How to challenge stigma around online abuse?
- What are the boundaries of acceptable/unacceptable technology use in the context of justice system?
- How to encourage reporting? How to improve trust in response and support from the police, government, and other agencies? What human-computer interactions can enhance trustworthiness of police practices?
- How to prevent surveillance during technology-enabled police investigations? Corporate and state online surveillance as a potential harm specifically to women and girls, that could turn into loss of freedom, for example through criminalisation of abortion—with health tracking and medical data being used as evidence.

**Revictimisation**

- How to disrupt cycles of revictimisation and multiple victimisation? What experiences and challenges contribute to revictimisation?

## 5. Policy Recommendations

As the national research centre with expertise in online harms and gender, we are committed to knowledge exchange and translation of research findings into policy insights. We have been engaging in with relevant stakeholders over 2022 through policy roundtables, seminars and the publication of the REPHRAIN Map of Online Harms.

Going forward, we are happy to support the regulatory and law enforcement bodies in the UK and internationally during consultations and evidence gathering activities. Please contact us at rephrain-centre@bristol.ac.uk if you would like to collaborate.

**Below we outline recommendations for policymakers, practitioners and law enforcement agencies.**

- An explicit inclusion of tech abuse/online harms against women and girls in risk assessment and safety planning frameworks used by law enforcement, support sector organisations, health practitioners etc. (i.e., The Domestic Abuse, Stalking and Honour Based Violence DASH);
- The annual reporting of online harms against women and girls in national statistics such as the Crime Survey England and Wales or through other relevant bodies such as Magistrate Courts and the Office for National Statistics;
- Systematic collection of data on women's and girls' experiences of online abuse / violence by the national statistics bodies, technology service providers and law enforcement agencies;
- The centralisation of police reporting routes which requires law enforcement to also update its fragmented crime recording system;
- For the police, an increase of technical expertise and capabilities (especially regarding forensics);
- For the key tech industry players, to submit evidence (e.g., to Parliament Committee) on the known historical and current prevalence of online harms against women and girls via their platforms/services/products and the actions they have taken;
- For digital literacy organisations, to address a gender gap in online safety, especially in the areas like dating, stalking, intimate partner violence;
- For the Medicines & Healthcare products Regulatory Agency, to improve the privacy and security of fertility/period trackers and other FemTech products to ensure user agency over storage of data, pseudonymisation or records, and third-party sharing;
- For the DSIT, to outline detailed guidelines for software developers, factoring in online safety and privacy. Such guidelines should specifically be cognizant harms pertaining underserved populations;
- For regulatory and law enforcement agencies (Ofcom, the Police Force and the National Crime Agency), to improve consistency in defining, measuring and reporting online harms experienced by women and girls;

- For regulatory stakeholders (e.g., Ofcom) and software developer community, to focus on proactively reducing the scope for perpetrators to abuse through devices rather than placing the responsibility on targets to adjust their behaviour in response to abuse;
- For the key stakeholders (e.g., domestic abuse charities, The National Police Chiefs Council), to understand the safety needs of vulnerable user groups and co-design codes of practice to be implemented by the developers