Consultation response:

Strategic Framework to End Violence Against Women and Girls & Foundational Action Plan for Northern Ireland

October 2023

Gender and Tech Research Group
University College London (UCL) Computer Science

Queens University Belfast (QUB) Institute of Electronics, Communications and Information Technology (ECIT)

Written Submission

Dr Leonie Tanczer
Adrianne Thompson
Coordinated by Jennifer Reed

Q10. Do you agree or disagree with our vision?

A. Agree

While we agree with the ambition of the vision, there is a risk that not **including technology-facilitated abuse within the definition of gender-based violence** will undermine the ability to realise it.

The current definition accounts for '*online abuse'* including cyberstalking and grooming – but "online" is a narrow term which does not account for the broader ways in which digital systems are being weaponised against women and girls.

The term 'technology-facilitated abuse' is more encompassing and reflective of the reality that many women and girls are facing. It is also more future proof, accounting for abuse through emerging technologies such as Internet of Things (IoT) devices.

Internet of Things (IoT) is an umbrella term for appliances and technologies which are 'smart.' Tanczer *et al* described them as 'the direct and indirect extension of the internet into a range of physical objects, devices, and products.[1]' This includes household appliances such as doorbells, speakers and other gadgets which have enhanced functionality such as video features and data collection. These devices are part of the fabric of everyday life for many people and they are here to stay, with estimates suggesting that there will be 125 billion IoT devices by 2030[2].

This technology has transformed the risk landscape for victim-survivors of domestic abuse by extending the reach of abusers - providing new methods by which they can harass, stalk, monitor, or abuse their victims without needing to be physically present.

IoT systems are basic, lack well-established security and privacy settings, and are designed on assumptions that all users trust each other. Perpetrators take advantage of this - such as accessing baby monitors to listen to private conversations, or remote activation of home appliances to **make victims feel that they are losing their mind (digital gaslighting**.[3]) Perpetrators, who usually control the settings, also take advantage of their greater understanding of the functionality to **underplay or exaggerate what the tech can do** – for example convincing their victim that they are able to watch them remotely all day to prevent them from seeking help.

As IoT devices are offering new ways for perpetrators to cause harm, the term technology-facilitated abuse or 'tech abuse' is increasingly being adopted. It features in the National Strategic Threat Risk Assessment (STRA) for Violence against Women and Girls[4], Statutory Guidance on Controlling and Coercive Behaviour[5] and the House of Commons Committee Report on Connected Tech[6] which called on the UK Government to make tackling tech abuse a priority. Including tech abuse in the definition of gender-based violence for Northern Ireland will therefore bring consistency with other parts of the UK, whilst helping future proof the framework.

Without this reference we only feel able to 'agree' with the vision and not 'strongly agree.' This is a theme throughout the consultation, where we agree with the intent but have not been able to wholly endorse the approach due to either an exclusion of IoT and tech considerations – or a lack of detail enabling us to understand whether this is / will be included in future.

---

[1] [40] Tanczer, L., Brass, I., Elsden, M., Carr, M., Blackstock, J.J., 2019. The United Kingdom's emerging internet of things (IoT) policy landscape.(2019). The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape. In R. Ellis & V. Mohan (Eds.), Rewired: Cybersecurity Governance

[2] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4508732

[3] ucl_g-iot_online_harms_tech_abuse_one_pager_-_feb2020.pdf

[4] https://www.vkpp.org.uk/publications/publications-and-reports/reports/strategic-threat-and-risk-assessment-of-violence-against-women-and-girls/

[5] Controlling or coercive behaviour statutory guidance (publishing.service.gov.uk)

[6] Connected tech: smart or sinister? (parliament.uk)

Q11. Do you agree or disagree that Outcome 1 will enable us to achieve this draft vision?

Outcome 1 - Changed Attitudes, Behaviours and Social Norms. Everyone in society understands what violence against women and girls is, including its root causes, and play an active role in preventing it.

A: Agree

We agree that Outcome 1 will help contribute toward achieving the draft vision, but this must include challenging stereotypes of what constitutes violence - including controlling and coercive behaviour and how it is facilitated.

The rise of smart home devices and IoT is impacting social norms. For example, parents using spyware to monitor their children's phones, or tracking their location through Snapchat or smart watches may normalise this type of behaviour to those young people as they become older and develop their own relationships[7]**. There is a risk that we further perpetuate the feeling that it is OK to be 'in' each other's lives and private spaces**, something the younger generation may already be more at risk of as they live their lives online.

Within the planned campaigns issues such as password sharing could be highlighted – showing that it should not be necessary for an individual to share their social media or device passwords with their partner, or how active bystanders can challenge this form of unacceptable behaviour.

Broader education around the risks of tech abuse must be carefully balanced, so that perpetrators of violence are not inadvertently upskilled into realizing there are new ways they can abuse their victim. Furthermore, institutional attitudes often trivialize tech-related abuse in comparison to physical harm. The study "Policing Technology-Facilitated Domestic Abuse: Views of Service Providers in Australia and the United Kingdom" from the Journal of Family Violence found that many victim-survivors perceive police as not recognizing technology facilitated abuse's severity as coercive control.[8]

For this reason, part of tackling tech abuse needs to be incorporating it into wider conversations around behaviours and norms. This includes challenging established notions that undermine its severity, shining a light on the range of risks that tech abuse presents[9] and humanizing how devastating the impacts of this form of abuse can be.

We would therefore recommend adding education on the potential misuse of IoT devices in domestic settings as part of the planned campaigns, including guidance on how to safeguard oneself against tech abuse and messaging which challenges behaviours associated with devices (such as password sharing, spying and location tracking.)

[7] https://www.frontiersin.org/articles/10.3389/fenrg.2021.765817/full
[8] https://link.springer.com/article/10.1007/s10896-023-00619-2
[9] https://www.ucl.ac.uk/computer-science/sites/computer_science/files/giot_policy_.pdf

Q12. Do you agree or disagree that Outcome 2 will enable us to achieve this draft vision?

Outcome 2 – Healthy, Respectful Relationships. Everyone in society is equipped and empowered to enjoy healthy, respectful relationships.

A: Agree

To equip everyone in society to enjoy healthy relationships, it is critical to fully account for the modern challenges of developing online relationships - and the role that tech plays in shaping them.

Young people are typically early adopters of new tech, so awareness of the implications and potential misuse of it within the context of gender-based violence is crucial – and should be delivered in both schools and community settings. Enabling them to deal with these issues goes beyond just awareness, it is also about understanding how to protect themselves and what to do if they do find themselves in an unhealthy relationship where tech is an exacerbating or enabling factor. **This needs to be accounted for within referral services,** especially as frontline services do not always feel able to respond appropriately to tech-related issues.

The planned research to map activity in the education sector, and scope emerging issues, must include tech abuse – and not just what we think of as conventional 'online' abuse. This could help identify the types of devices through which young people are experiencing abuse, such as games consoles, a level of detail which can inform follow up action including evidencing issues with the manufacturers.

Q13. Do you agree or disagree that Outcome 3 will enable us to achieve this draft vision?

Outcome 3 – Women and Girls Are Safe and Feel Safe Everywhere. Organisations and institutions across government and society embed the prevention of violence against women and girls in all that they do so that women and girls are safe and feel safe everywhere.

A: Agree

We agree with the ambition to ensure that women and girls are safe and feel safe everywhere and welcome the recognition that this includes online spaces. However, as IoT devices can be found everywhere, from public places to private homes, the section should also address the implications they hold for violence against women and girls.

We would recommend including a **commitment within the Action Plan to introduce guidelines for (i) securing IoT devices in public spaces to make them safer** for women and girls and (ii) **safe IoT usage to give women and girls more confidence as part of the media literacy strategy**.

Collaboration with, or stricter regulation for tech companies should also be included to ensure that safety for women and girls is factored into product design, and specific risks posed by IoT are accounted for in safety policies and procedures (see response to Q16.)

The framework recognises that online abuse inhibits women and girls from expressing themselves in online spaces and restricts how they can participate in public life. Our research has shown that this also applies to broader tech abuse, such as that facilitated by IoT. This issue is exacerbated when there is an expectation placed on the victim that they change their behaviour, such as

suggesting they come off social media[10] or delete certain apps, as opposed to **challenging the perpetrator's behaviour.**.

IoT can play a significant role in aiding women and girls to regain a sense of security following a domestic abuse relationship. At this recovery stage, many women find solace in the protective measures certain devices offer, such as home security cameras, video doorbells, and mobile phones. Notably, the use of mobile phones equipped with GPS location services offers women an additional layer of safety, allowing them to share their whereabouts with trusted individuals or alert authorities promptly. The distinction lies in the **victim/survivors' comprehension of the technology and retaining autonomy over its use**,[11] a key tenet when considering how women and girls can feel and be safer.

14. Do you agree or disagree that Outcome 4 will enable us to achieve this draft vision?

Outcome 4 – Quality Frontline Services, Protection, and Provision for Victims and Survivors of Violence Against Women and Girls. Provision of high-quality services for women and girls who are victims and survivors of violence against women and girls.

A: Agree

Women and girls experiencing domestic abuse face the greatest level of risk when seeking to leave or leaving their relationship[12]. This is the phase where most homicides occur, and when providing inaccurate advice and support could put the victim at increased risk or danger – such as advice which does not adequately consider the implications of IoT devices.

Frontline services must include IoT and other emerging technologies as part of their risk assessment process and be able to access specialist advice on what steps to take, if needed. Risk assessments currently focus too narrowly on the most commonplace devices, such as a phone, laptop or tablet. Even with these devices, **if there is not an understanding of the different ways that IoT risks can manifest, incorrect advice may be given**. For example, advising a victim to delete spyware from their phone when they are not yet able to leave the relationship, can alert the perpetrator that the victim has sought help.

Similarly, **a narrow focus on common devices like phones and tablets misses the bigger picture – and the potential risks posed by other devices**. AirPods and smart watches for example could provide a way for the perpetrator to continue to track the location of the victim/survivor once they leave. Using apps such as Uber or shopping delivery apps could all potentially give information to the perpetrator about where the victim/survivor is located if they have access to the same accounts. Devices owned by immediate family members could pose a similar risk, such as children's devices, who they speak to on video games, or AirTags placed in children's toys.

Adequate risk assessment is only the first piece of the puzzle. Staff in frontline services also need **training to understand how tech abuse manifests so that they know how to spot issues and patterns of abuse**. This is not limited to frontline staff in domestic abuse services, GPs for

[10] https://committees.parliament.uk/oralevidence/10627/pdf/
[11] https://read.dukeupress.edu/demography/article/59/2/653/294668/Safer-If-Connected-Mobile-Technology-and-Intimate
[12] Matthews et al 2017, 'Stories from survivors: Privacy and security practices when coping with Intimate Partner Abuse' https://dl.acm.org/doi/pdf/10.1145/3025453.3025875

example can be supported to identify this type of abuse[13] – particularly with cases involving healthcare apps or devices including cochlear implants and insulin pumps.

Consideration must also be given to the context within which domestic abuse advisers operate. They must already understand housing issues, legal factors, account for mental health, a whole plethora of complex considerations – do we also now expect them to complete become tech experts? Their training **must be complemented by access to tech specialists (such as through a dedicated helpline[14]) and central resources which are able to support with complex cases and keep on top of technological developments**.

We would welcome IoT being an early focus for the agile working groups, and its specific inclusion in the planned gap analysis for frontline services. This should include capability to assist with technologically involved abuse cases in Northern Ireland and routes to specialist advice within an ever-evolving tech landscape.

15. Do you agree or disagree that Outcome 5 will enable us to achieve this draft vision?

Outcome 5 – A Justice System which has the Confidence of Victims, Survivors and the Public in its Ability to Address Violence Against Women and Girls. In the context of violence against women and girls, a justice system that considers and addresses the needs of people who come into contact with it, holds perpetrators to account, while challenging and supporting them to change, gives victims and survivors a voice and a place in the process, and has the confidence of the public.

A: Agree

Police are key first responders to domestic abuse, and research[15] has begun to uncover shortcomings in police responses to tech abuse, **yet there is no detail in the strategic framework on the role they will play**.

A recent survey[16] of domestic abuse service providers showed a perception of **bias amongst the police towards physical forms of abuse, and that they are likely to dismiss or trivialize non-physical abuse** – such as disregarding text messages as 'not real[17]' evidence, or failing to recognise controlling and coercive behaviour when it is facilitated by tech.

Inadequate training is contributing to this (including for cybercrime teams who are not by default trained in domestic abuse) as is insufficient time and personnel to tackle TFDA, and issues associated with evidence collection. To address domestic abuse in the digital age, each of these underlying issues must be addressed, and the strategic framework offers an opportunity to make a commitment on this. There is some promising work which can be drawn on, such as the

---

[13] Straw, I., & Tanczer, L. (2023). **Safeguarding Patients From Technology-Facilitated Abuse in Clinical Settings: A Narrative Review**. PLOS Digital Health, 2(1), e0000089. Publication available here

[14] Tanczer, L., Lopez-Neira, I., Parkin, S., Patel, T., & Danezis, G. (2018). **Gender and IoT Research Report: The Rise of the Internet of Things and Implications for Technology-Facilitated Abuse. London: STEaPP, PETRAS IoT Hub. Publication available here. And;**
Burton, S., Tanczer, L., Vasudevan, S., & Carr, M. (2021). **The UK Code of Practice for Consumer IoT Cybersecurity: Where we are and what next. PETRAS IoT Hub, Department for Digital, Culture, Media & Sport (DCMS): London. Publication available here**

[15] Flynn et al., 2023; Tanczer et al., 2021; Woodlock et al., 2022

[16] Douglas, H., Tanczer, L., McLachlan, F. *et al*. Policing Technology-Facilitated Domestic Abuse (TFDA): Views of Service Providers in Australia and the United Kingdom. *J Fam Viol* (2023)

[17] Harris & Woodlock, 2022

trialling of an app by Greater Manchester Police[18] that allows police to collect evidence from the victim/survivor's phone at the scene of the incident or time of the report, speeding up processes while enabling the victim/survivor to retain their phone.

Domestic abuse agencies have evidenced that tech abuse features in the majority of cases they see[19]. **Collecting data on tech abuse and IoT within police reports and official crime statistics will broaden the evidence base and help inform future activity** to tackle this threat. It may also help conceptualise and solidify the issue within the Police force, reinforcing the prevalence of this issue and how it manifests.

The Domestic Abuse and Civil Proceedings Act (Northern Ireland) 2021 is a significant stride towards addressing the multifaceted nature of domestic abuse. Courts in Northern Ireland should invoke its provisions more frequently, by consistently applying the domestic abuse aggravator, the judiciary can underscore the gravity of both physical and tech-enabled abuse. Emphasizing this legislation not only aligns with the changing landscape of intimate partner violence but also signals a commitment to robustly address and penalize such behaviours. Regular use of these provisions would establish a precedent, ensuring victims/survivors receive justice while deterring potential perpetrators and elevating the discourse around domestic abuse.

Ensuring perpetrators are held accountable for their actions should include the actions those they undertake online or through devices. **Perpetrator education programmes**, currently a blind spot for tech abuse, could be used to challenge behaviour and ensure the onus for change is on the perpetrator and not the victim/survivor.

Q16. Do you agree or disagree that Outcome 6 will enable us to achieve this draft vision?

Outcome 6 – All of Government and Society Working Better Together to End Violence Against Women and Girls. A whole system approach with collaboration and cooperation by default across government departments and with, within and between the community, voluntary and other sectors.

A: Agree

IoT specific stakeholders and IoT implications should be included in future governance arrangements such as advisory groups, boards, or working groups.

It is also essential to **incorporate IoT misuse into the new data strategy with IoT-specific metrics and indicators**, and an inclusion of disaggregated data to help plug gaps – which can be identified through new, comprehensive data mapping. Tech abuse data must then be published and reported on to understand the extent of digital threats, monitor impact of interventions and ensure accountability.

The Framework should also commit to introducing a new statutory duty of care on tech companies to keep their users safe from coercive and controlling behaviour and other forms of abuse (including digital gaslighting) and ensure they are proactive in addressing potential misuse of their products[20] in the context of gender-based violence.

---

[18] Greater Manchester Authority, 2022

[19] Suzy Lamplugh Trust 100% of cases have cyber element 72% of Refuge service users identify experiencing tech abuse - Refuge

[20] Leonie Tanczer - Gender and IoT: The implications of IoT on Victims/Survivors of Gender-Based Domestic Violence and Abuse

A package of minimum requirements should be established to ensure consistency and adherence with this new duty, which, as our research has shown, should include -

a) **Notifications to alert users** when their device is being used to track or monitor them (e.g. through spyware)
b) **Provide resources with advice and guidance** on IoT safety, with clear information about functionality and how personal data is collected (and explore links to new media literacy approach)
c) **Dedicated services and means to report incidents** of harassment and tech abuse, including offline options such as print / helplines.
d) **Collect data** on incidents of tech abuse to understand the nature of the problem and assess emerging threats in real time. Explore how this can be shared with Government and frontline services to inform and shape prevention activity.
e) **Collaboration** with tech-focused NGO's, advocacy groups, academia, frontline services – within the proposed knowledge transfer programme. Focus could include sharing insight, undertaking joint research, curating and sharing resources, conceptualising innovative ideas on user safety, jointly developing tech-related policies and regulations such as setting safety standards, promoting transparency and awareness, feeding into training sessions for domestic abuse advisers.
f) **Introduce preventative measures within product design, including easy to use tools for users to take control of privacy and visibility of account settings** – such as who has access to it, regular notifications that you are still logged in other devices, new standards for 'safe use' features, and clear instructions for all IoT devices.

By integrating these recommendations, the strategic framework will not only address traditional means of violence and abuse, but also proactively and effectively address the unique challenges posed by the Internet of Things.

Q17. Do you agree or disagree with our approach of focusing on PREVENTION to end violence against women and girls?

A: Agree

The type of abuse we see committed through IoT is not new. Typically, it includes stalking, harassment, gaslighting, and coercive or controlling behaviour. What IoT devices do, is offer a new tool for facilitation of this abuse – a means of extending the reach of perpetrators, and new methods which mean they no longer need to be physically with or close to the victim/survivor. **The prevention approach focuses on stopping violence before it occurs. By tackling risks posed by IoT there is an opportunity to stop perpetrators at source from being able to weaponize devices as a tool for violence**.

Within questions 10-16 we have incorporated our responses related to prevention specific to each outcome, such as tackling social attitudes to prevent normalisation of acts like location tracking and password sharing, educating on the risks of IoT and how to use devices safely, and improved product design. We have also recommended **data collection to identify emerging threats related to IoT and tech abuse, so that these can be tackled in a preventative way**. There will need to be consensus around how tech abuse is defined and measured. We have recently launched a piece of research on this and would be happy to share further details if helpful.

Q18. Do you agree or disagree that these are the right actions to take in our draft Foundational Action Plan?

A: Disagree

While we agree with the ambition of the plan and the fundamental principles, **the risks that IoT pose in the context of gender-based violence are not captured within the action plan or accounted for**. We have made recommendations (Q10-16) which would address this.

Q19. Do you agree or disagree with the way the Equality Impact Assessment (EQIA) has been carried out; (Q20) do you agree or disagree with the findings?

A: Agree

The EQIA shows detailed consideration to the implications of the framework and action plan. Ahead of the Decision Report being published, and as part of future EQIA reviews, we would welcome consideration of the following points;

a) **Recognition of the data gap around tech abuse and granularity on how IoT has facilitated the reported crimes**. Statistics provided in EQIA show that 64% of females have experienced sexual harassment, but there is no further detail on whether or not this was facilitated by tech. Where tech considerations are captured in data they are minimal, such as only asking about text messaging. The EQIA has sought to use qualitative outputs to plug data gaps, and future EQIA's should consider using this approach to build an appropriate picture re tech abuse whilst data capability is built.
b) **The EQIA notes that psychological violence and coercive control are not being taken seriously in Northern Ireland**[21], and there is a relatively low feeling amongst young males (41%) that virtual or online abuse of a partner is an example of domestic violence. This reinforces the need for education about the severity of tech abuse and tackling social norms among young people.
c) There were also a small number of women who felt the police had showed a lack of empathy or tried to discourage them from taking their case forward. It would be useful to understand whether these were instances related to tech abuse, and if this were a contributing factor to why it was trivialised.
d) As the EQIA explores mitigations for sections of society who may face barriers due to literacy, consider **extending this to technological and media literacy** – particularly as these imbalances are taken advantage of by perpetrators of domestic abuse.
e) In designing actions to tackle cultural and stereotypical attitudes and prevent victim-blaming in some religious communities where there is an interpretation of 'improper' behaviour, consider how tech can exacerbate this – such as deepfake imagery being used as blackmail.
f) We have set out in our consultation response the need for offline options for women and girls to access support and advice, such as print and helplines, where their devices are compromised. Consideration of how homeless women and girls can access offline resources should also be undertaken, particularly where they are homeless as a result of domestic abuse.

[21] Doyle, J., & McWilliams, M. (2018). Intimate Partner Violence in Conflict and Post-Conflict Societies: Insights and Lessons from Northern Ireland

Summary

Section	Recommendation
Vision	1. Broaden definition of Gender-Based Violence to include Technology-Facilitated Domestic Abuse, reflecting the broader reality in which tech is being weaponised against women and girls – including through Internet of Things (IoT) devices and digital gaslighting.
Outcome 1	2. Include education on the potential misuse of devices in domestic settings as part of the planned campaigns and incorporate tech abuse into wider activity which will challenge the stereotypes underpinning unacceptable social norms.
Outcome 2	3. Include tech abuse (not just conventional 'online' abuse) in planned research activity to map activity, and emerging issues, in the education sector 4. Educate, in schools and community settings, young people on the potential misuse of tech within the context of gender-based violence - and ensure they are able to access support within referral services if needed.
Outcome 3	5. Introduce guidelines for (a) securing IoT devices in public spaces to make them safer for women and girls and (b) safe IoT usage as part of the media literacy strategy. 6. Ensure that relevant advice and guidance on IoT safety and tech abuse supports women and girls to stay online and connected, with onus of behaviour change on the perpetrator.
Outcome 4	7. Frontline staff should be trained to understand how tech abuse manifests to enable them to identify occurrences, and services must capture IoT and other emerging technologies as part of their risk assessment process - and be able to access specialist advice when needed through provision of central resources and a dedicated helpline. 8. IoT should be accepted as an early focus for agile working groups, and included in the planned gap analysis for frontline services
Outcome 5	9. Set out within the Framework the role that the police will play in contributing to Outcome 5, and how underlying issues including inadequate training (extending to cybercrime teams) insufficient time, and issues with evidence collection will be tackled. 10. Introduce mandatory capture of tech abuse within police reports for domestic abuse cases, utilise data to inform police approach and publish within crime statistics.

	11. Explore how tech abuse can be incorporated into perpetrator education programmes
Outcome 6	12. Include IoT specific stakeholders and IoT implications in future governance arrangements such as working groups and boards. 13. Incorporate IoT misuse into the new data strategy with IoT specific metrics and indicators and an inclusion of disaggregated data, to be published and reported on. 14. Introduce a new statutory duty of care on tech companies to keep their users safe from abuse, to ensure they are proactive in addressing potential misuse of their products in the context of gender-based violence. Minimum requirements should include; a) **Notifications to alert users** when their device is being used to track or monitor them (e.g. through spyware) b) **Provide resources with advice and guidance** on IoT safety, with clear information about functionality and how personal data is collected c) **Dedicated services and means to report incidents** of harassment and tech abuse, including offline options such as print / helplines. d) **Collect data** on incidents of tech abuse to understand the nature of the problem and assess emerging threats in real time. Explore how this can be shared with Government and frontline services to inform and shape prevention activity e) **Collaboration** with tech-focused NGO's, advocacy groups, academia, frontline services – within the proposed knowledge transfer programme. f) **Introduce preventative measures within product design,** including easy to use tools for users to take control of privacy and visibility of account settings
EQIA	15. Ahead of the Decision Report, and as part of future EQIA reviews; a) Recognise the data gap in relation to tech abuse, b) Analyse further cases where police lacked empathy, to understand whether tech abuse may have been a contributing factor, c) Consider how technological and media literacy may create barriers for women and girls d) Consider how tech might be weaponised differently for specific types of abuse, such as so called 'honour-based' abuse e) Ensure offline options are available to women and girls to access support and advice, including those who are homeless.

ucl.ac.uk/computer-science/research/research-groups/gender-and-tech

qub.ac.uk/ecit