None
Internet-Draft
Intended status: Informational
Expires: 7 May 2026

S. Celi
Brave
J. Guerra

M. Knodel
CDT

3 November 2025

Intimate Partner Violence Digital Considerations
draft-irtf-hrpc-ipvc-02

Abstract

This document aims to inform how Internet protocols and their implementations might better mitigate technical attacks at the user endpoint by describing technology-based practices to perpetrate intimate partner violence (IPV). IPV is a pervasive reality that is not limited to, but can be exacerbated with, the usage of technology. The IPV context enables the attacker to access one, some or all of: devices, local networks, authentication mechanisms, identity information, and accounts. These security compromises go beyond active and passive on-path attacks [RFC7624]. With a focus on protocols, the document describes tactics of the IPV attacker and potential counter-measures.

Discussion Venues

This note is to be removed before publishing as an RFC.

Source for this draft and an issue tracker can be found at https://github.com/claucece/draft-celi-ipvc.

Status of This Memo

This Internet-Draft will expire on 7 May 2026.

Table of Contents

1. Introduction

Intimate partner violence (IPV) refers to physical, emotional, verbal, sexual, or economic abuse of a person by a current or former intimate partner, hereafter referred to as the abuser or attacker.[WHO] IPV is characterized by an unequal power dynamic that enables the abuser to exert control and harm within romantic or sexual relationships context. While IPV often manifests in these contexts, it also extends to child and elder abuse or abuse perpetrated by any member of a household.

Digital technologies are central in modern lives and can be used as a way to enable and enhance IPV. Technology-based IPV has profound implications on the physical, psychological and emotional health of survivors, affecting them not only at the individual level but also disrupting their broader social environment [ref]. Furthermore, technology-based IPV can create an immediate potential for offline, real-world harm, as attackers can use these methods to control, locate, or confront their victims in person. This blending of digital abuse and offline harm increases the severity and urgency of the threat faced by victims.

Unlike traditional "attackers", an abuser in the context of IPV is a close and familiar figure: an "attacker you know." This attacker is neither solely on-path nor off-path; they often have full access to their target’s devices and local networks, sharing intimate spaces and information. Moreover, abusers can coerce and manipulate their victims (hereafter, referred to as targets) directly.

There is significant existing work in the field of online gender-based violence [IPVTechBib][CSP] and technology-based IPV [Freed] mainly focused on response and resiliency, including digital privacy and safety strategies. Nevertheless, even when this literature exists, IPV is not considered enough when designing digital technologies, networks, or Internet protocols, and it is not part of threat-modelling. Protocol design or cybersecurity best practices rarely account for IPV-specific scenarios, as seen in only a few cases [CETAStrategies]. These omissions highlight the need to consider the privacy and security risks involved, as noted in [RFC6973].

This document outlines the tactics employed in technology-based IPV and offers recommendations for designing protocols and technologies to mitigate these tactics. It begins with a comprehensive overview of IPV and related terminology, followed by an exploration of the specific tactics used by abusers, culminating in actionable recommendations for the digital design community.

Although the category of technology-abuse includes practices such as Child Sexual Abuse Material (CSAM), or digital manipulation of images and videos (deepfakes) to exhibit and slander women [Witness], those tactics are out of scope in this document, since the attacker is not part of the victim’s close social environment, i.e. they do not necessarily have access to the victim’s local network. However, in some occasions, this distinction doesn’t always hold.

The point of this document is to describe technological means by which abuse may be enacted. It is not claiming, and cannot claim, that these means are inherently abusive.

2. Definition of technology-based IPV

Technology-based intimate partner violence (IPV) refers to the use of digital tools and technologies to enable, escalate, and reinforce abusive behaviors. IPV itself encompasses physical, emotional, verbal, sexual, or economic abuse committed by a current or former intimate partner. A "partner" in this context is not limited to romantic or sexual relationships, but can extend to anyone with a close relationship to the victim, including household members involved in child or elder abuse (however, here we will not explictly consider this case). What defines IPV is the inherent unequal power relationship, where the abuser leverages this imbalance to inflict harm and exert control.

In technology-based IPV, the attacker exploits various forms of digital technology to perpetrate abuse, often through pervasive surveillance, overt monitoring, coercive access to devices or accounts, and manipulation of digital communications. This is known as "digital coercive control" [Dragiewicz2018], which is a form of abuse where access to personal technology, such as smartphones, social media, or local networks, becomes a means for the abuser to assert control, engage in stalking, or inflict psychological harassment. Internet-enabled technologies amplify the abuser’s ability to conduct continuous surveillance or escalate harm remotely, reinforcing the unequal power dynamic present in IPV situations.

While technology-facilitated abuse can affect anyone, it is crucial to recognize its intersection with gender-based violence. As noted by [APCFramework], "women and girls face specific cyber threats in the digital age that are considered forms of gender-based violence as they occur because of their gender, or because they disproportionately affect one gender." This intersection arises because digital abuse is embedded in the same offline structural violence that perpetuates gender inequality, but the technological dimension introduces new elements: searchability, persistence, replicability, and scalability. These features allow abusers to more easily track their targets, replicate abusive content, and escalate harassment across platforms, magnifying the harm inflicted.

Furthermore, the unique aspects of technology-based IPV— such as the ability to monitor in real-time, manipulate social media, or restrict access to digital resources— can severely limit a victim’s autonomy and mobility. This creates a new layer of control that extends beyond traditional physical spaces into the digital realm, making it harder for victims to escape the abuse, as the attacker often has constant or even remote access to the victim’s digital life.

Ultimately, technology-based IPV is not just an extension of traditional abuse; it is an evolving form of violence that capitalizes on the pervasive and intimate nature of digital technology to create a form of control that is difficult to detect and even harder to escape. Addressing this issue requires a deep understanding of both the technical tools used by abusers and the social dynamics at play, including the broader structural inequalities that enable such abuse.

2.1. Terminology

In the rest of this draft, we will use this terminology:

Attacker: A person who, in the context of intimate partner violence (IPV), uses digital tools to exert control, monitor, or harm another individual with the aim of enabling or enhancing abuse. The term "attacker" is used interchangeably with "perpetrator." * Victim: By "victim" we mean a person who is subject or target of an attack. Notice that we are using this term only in the temporary context of an attack scenario. We prefer the term "survivor", which recognizes the agency and resistance tactics of those facing IPV, but for the purposes of this document we focus on the fact of being subject of specific technology-based IPV attacks.

3. Technology-based IPV attacks

In this section, we describe IPV attacks that are enabled or exacerbated by Internet technology. First, we outline our assumptions about this type of attacker and common tactics they may use. Then, we describe the types of technology-enabled IPV attacks.

3.1. The tech-asisted IPV attacker

The attacker we focus on in this document is someone who either forcefully controls accounts, devices, and/or authentication information used to access systems, or leverages publicly available information to exert this control. This attacker may or may not be technologically skilled (it might be "technology savvy" or not). From a threat model perspective, this attacker is one of the strongest ones as it can use their abilities to gain unlimited access to systems and devices without needing significant financial or computational resources.

The attacker typically has (or has had) physical access to the victim and often shares a common social network with them. In some cases, the attacker may legally own the devices or accounts the victim uses, further complicating the victim’s ability to maintain control.

The attacker is not implied to have infinite computing power or unrestricted access to external systems (e.g., companies' infrastructure). Rather, the focus is on their ability to gain unlimited access to the victim's personal devices and accounts due to their proximity, control, or manipulation of the victim's authentication mechanisms and personal data, communications, and digital assets..

3.2. Tech-based IPV tactics

There are many ways in which digital and networked technology can facilitate an attacker perpetrating IPV. For an in-depth reading, see [TBMDGMMDR] and [CDOHPFLDMR]. Below, we informally categorize the main tactics attackers use:

* Ready-made tools: Attackers can use applications or devices that are solely built to facilitate IPV. These types of technology are sometimes referred to as "stalkerware" or "spouseware".

* Dual-use tools: Attackers can repurpose applications, settings or devices built for beneficial or innocuous purposes to cause harm. This is the case, for example, of anti-theft devices that can be repurposed for stalking, or to location-tracking tools. The latter is subject to its own considerations [DULT].

* Impersonation attacks: Knowing personal information coupled with access to authentication mechanisms gives an attacker the ability to fully authenticate to services and accounts of the victim, effectively impersonating them. This can be executed to the degree that the victim can no longer successfully authenticate themselves to their services or accounts.

* UI-bound impersonation attacks: Attackers can abuse technology to enhance IPV by abusing the User Interface (UI) of a specific tool. In this case, attackers become authenticated but adversarial users of a system. They cannot, however, escalate to root privileges or access other underlying functionalities of the system. They are bound to the UI of whatever system they managed to authenticate to. We will explore later the ways attackers use to forcibly gain authentication to a system.

* Social media and forums: Attackers can learn and share information on how to use technology to enhance IPV through the usage of these platforms. These spaces may also provide narrative justifications for abusive behavior and facilitate cyberstalking, cyberbullying, and doxxing.

* Perception of Threat and Vulnerability: The awareness of a pervasive threat can act as a powerful form of control. Attackers often leverage the perception that technology could be used for IPV as a means of manipulating victims, eroding their sense of safety and agency. This can extend to perceptions of vulnerability within the victim's network or system: the mere suspicion of a vulnerability could compound feelings of insecurity. Research on user perceptions of technology trustworthiness, especially within messaging apps (see [UPMSG]), indicates that perceived threats and vulnerabilities in communication channels can discourage users from trusting or seeking help through these technologies. Such dynamics can further isolate victims and create additional barriers to receiving support.

3.3. Kinds of tech-enabled IPV attacks

The attacks we list and are discussed in this document exploit the tight integration between personal technology and everyday life, leveraging access to accounts, devices, authentication mechanisms, and personal or sensitive information. The examples below illustrate, but are not limited to, common categories of tech-enabled IPV. Each represents a distinct vector through which an attacker can extend coercive control, surveillance, or isolation, often combining multiple tactics at once.

* Monitoring: A prevalent tactic to facilitate IPV is the active, intrusive monitoring of the victim's online activities and accounts. This ongoing surveillance can encompass a range of behaviors that feel invasive, often involving threats or intimidation. The "active" nature of this monitoring means it may be apparent to the victim or entirely hidden, depending on the abuser's intent. Forms of monitoring include:

  - Monitoring of communication, which can be e-mail-based, chat-based or social media communications, or browsing information (history, cookies or more) either directly on the victim's device or through specialised applications.

  - Monitoring location and whereabouts by looking at the metadata of communication, by using location-help applications, or by using specialized applications.

  - Monitoring any data sent over the network by mounting DNS attacks or other specialised attacks.

  - Monitoring any information found on the UI by looking at devices screens while the victim is using them.

- Data gathering by using the Internet to seek public or private information to compile a victim’s personal information for use in harassment.

- Monitoring security cameras or systems for home security

In this type of attack, we see these dimensions:

- Monitoring of communication content at various layers, including the application layer (e.g., chat or email content) and network layers (e.g., packet inspection or traffic analysis).

- Monitoring of the UI content of application tools.

- Monitoring of location information.

* Compromise of accounts: An attacker may demand access to the victim’s accounts to continuously monitor, control, manipulate or restrict their digital communications and activities. Unlike passive monitoring with publicly available tools, the attacker demands access to tools and contents in order to reduce the "life space" or "space for action" that the victim has for independent activities. Once access is obtained, an attacker can:

  - Delete data, which can be communication data, documents and more (essentially, any data stored in the account).

  - Gain access to contacts such as friends, family or colleagues.

  - Gain access to communications, audio-video content, and any associated metadata.

  - Modify or manipulate any communications, audio-video content, and any associated metadata.

  - Lock out or change the authentication mechanisms that grant access to the account.

  - Impersonate the victim by using the victim’s online identity to send false/forged messages to others or to purchase goods and services.

  - Impersonate the victim by using the victim’s online identity to publicly post information that can be private or fake, impacting their reputation and sense of security.

- Impersonate the victim by using the victim’s online or legal identity to sign victims up for services.

- Exposing private information or media by distributing intimate or private data (which could have been acquired via coercive tactics).

* Compromise of devices: This attack is similar to the above, but the attacker demands access to the victim’s devices. The goal is the same as the above but the result is more impactful, as it restricts access and gives access to accounts that are accessed through the device. It can also prevent the victim from having any connection to the Internet. Once an attacker has access to the device, they can use it to:

  - Physically prevent the use of the abilities given by the device (the device can be used, for example, to call police services, which is restricted with this attack).

  - Access contacts and data (media or messages) stored in it.

  - Access to accounts and authentication mechanisms for other accounts (saved passwords or authenticator apps -2-factor authentication-, for example).

  - Perform impersonation.

  - Perform denial of access to the device, networks or the Internet in general.

  - Destroy the device itself and any information stored in it.

  - Impersonate by using the victim’s online identity, as accessed through the device, to publicly post information that can be private or fake.

* Exposing Private Information or Media: This attack often builds on other the forms of attack. Once an attacker gains access to an account or device, they can harvest sensitive data, including personal and/or private media, messages, and private documents. This stolen information can then be used to threaten, extort, or humiliate the victim. For example, intimate images may be used for blackmail, or private details such as bank account and tax information may be exploited. The attacker may also engage in doxxing by publicly sharing private details to damage the victim’ s reputation or relationships.

* Denial of Access: This attack can also be built upon previous ones, and its objective is to block the victim’s access to essential services. It can include physical measures such as destroying routers or network devices, changing Wi-Fi passwords, or modifying network settings. This prevents the victim from connecting to the Internet or accessing online services. Denial of access may also target financial abuse, such as restricting the victim’s access to online banking or digital wallets, making it difficult or impossible for them to manage their finances. Denial of access can also extend to digital communication disruptions, such as flooding the victim’ s communication platforms with unwanted messages or deploying viruses to compromise their devices. The goal is to isolate the victim, severing their connection to the outside world, including family, friends, and support networks.

* Threats: Often intertwined with denial of access, threats involve sending harassing or abusive messages via email, chat, or social media. These messages may include insults, intimidation, or direct threats of harm. The purpose is to instill fear, destabilize the victim’s emotional state, and force compliance, either by causing distress or pushing the victim toward further harmful actions. Threats can escalate into more severe attacks, including denial of access or exposure of private information.

* Harassment: Harassment can be anonymous, but in many cases, the victim knows the identity of the attacker. However, due to the anonymity of certain platforms, the victim may struggle to hold the perpetrator accountable. The systems in place often require that harassing content be permanently available for investigation, but this can, in turn, prolong the victim’s exposure to the abuse. Harassment can manifest in various forms and dimensions:

  - Ongoing Harassment: This type of harassment is persistent, with the goal of intimidating, humiliating, and psychologically tormenting the victim. It often involves repeated messages, threats, or actions that make the victim feel unsafe or violated.

  - Post-Disconnection Harassment: Once the attacker no longer has physical control over the victim, they may resort to cyberstalking or continued harassment online. This form of abuse allows the attacker to maintain control over the victim by stalking their digital presence, often through social media, messaging platforms, or by monitoring their activities in other ways.

3.4. Means of attacking

The attacks described above can be carried out using various methods. Below are some of the most common approaches:

* Spyware Installation and Spoofing: This method involves installing malicious software on the victim’s device to gain unauthorized access to their accounts or to conduct active monitoring. It may also include spoofing techniques to bypass security measures, such as remotely compromising security questions, passwords, or other authentication methods. These tools are typically installed without the victim’s knowledge, giving the attacker covert access to their personal information.

* Coercion and Control: This form of attack leverages physical, emotional, or psychological manipulation to gain access to a victim’s devices, network credentials, or digital information. It often involves forcing the victim to reveal sensitive details, such as passwords, PINs, or authentication mechanisms for their accounts and devices, creating an environment of control and fear.

* Shared Network Plans and Account Ownership: In some cases, an attacker may be the legal owner of a device (e.g., a parent’s control over a child’s device) or have access to shared family accounts or network plans. For instance, an abuser may control a joint bank account or device within a shared family plan, allowing them to carry out attacks without the victim’s knowledge and without needing to install malicious software.

* Monitoring: This method involves the exploitation of social media and other publicly available information to track the victim’s activities. It may also include the installation of monitoring tools on the victim’s devices or the abuse of "benign" applications (e.g., location-tracking apps) in a malicious way. The attacker uses these tools to keep tabs on the victim’s movements and interactions, often in secret.

* Exposure: This method involves the use of social media platforms to amplify harassment. It includes actions such as posting harmful content to embarrass, humiliate, or intimidate the victim, or sharing private information like intimate images without consent. This form of attack may also involve doxxing, where the victim’s personal details are shared publicly to cause distress or harm to their relationships and reputation.

4. Specific abused technology

Research into how attackers exploit technology to enhance IPV reveals that the following technologies are frequently abused:

* Passwords and Authentication Mechanisms: Authentication systems are often the primary point of failure in IPV attacks. Once an attacker gains access to a victim’s account or device, they can use that access to compromise additional accounts or devices. Attackers can use specialized tools, often installed surreptitiously on the victim’s device, to capture authentication data. They may also coerce victims into revealing passwords or bypassing security features. This includes targeting biometrics (e.g., fingerprints, facial recognition), two-factor authentication (2FA) systems, and other multi-layered security methods.

* Media and Private Information: Attackers who gain access to devices or accounts can harvest private media and sensitive personal information. This data can then be used to extort the victim, humiliate them (by sharing it publicly), or escalate harassment. Private communications, photos, and other intimate materials are particularly vulnerable to such exploitation, often used as leverage in controlling or threatening the victim.

* Account Recovery Mechanisms: In addition to direct access to authentication mechanisms, attackers can manipulate account recovery processes to gain unauthorized access to accounts. This includes exploiting weaknesses in 2FA devices, recovery email systems, or password reset tools. By compromising these systems, attackers can gain control over multiple online profiles, furthering their ability to surveil and control the victim.

* Lack of Blocking Mechanisms and Exploitation of Anonymous Channels: Many platforms and communication tools lack effective blocking or reporting mechanisms, which attackers exploit to continue their abuse. Common tactics include:

  - Using fake phone numbers or burner accounts to contact the victim.

  - Sending messages via platforms with open channels that do not require mutual consent (e.g., messaging apps with open chat features).

  - Exploiting "read receipts" or similar features to monitor the victim’s engagement with their messages, thereby gaining further control.

- Abusing the absence of robust blocking features to maintain constant contact and harassment.

5. Recommendations

The following recommendations are tailored for protocol and systems designers to help mitigate technology-enabled IPV, recognizing that IPV often occurs within the broader context of structural violence (which can be gender-based violence). While these attacks are facilitated or exacerbated by technological tools, the recommendations focus on enabling victims to regain control, prevent the abuse of power, and limit attackers' ability to carry out actions that entrench their control.

* Build proper authentication systems: Authentication mechanisms should be designed with the following features:

  - Account Access Transparency: Maintain a non-deletable and non-modifiable list of devices with access to accounts and a record of active sessions.

  - Recovery and Revocation: Provide secure ways to recover access to accounts and change authentication mechanisms. Allow easy revocation of access, including when an account or device is compromised.

  - Clear Notifications: Send notifications when:

    o New devices are used to access an account.

    o Attempts to access accounts occur.

    o Changes are made to account details.

  - Approval Mechanism for Access: Implement a system that allows users to approve or deny access attempts from new devices or locations.

* Storage and sharing of media: Media should be handled in a way that allows the victim to retain control:

  - Media Takedown: Ensure that private media posted without consent can be taken down at the victim's request.

  - Dealing with Re-posting: Implement mechanisms to prevent re-posting of previously reported non-consensual media, either by blocking its sharing or by flagging it across platforms and devices.

- Secure Reporting Mechanisms: Provide private, confidential ways to report non-consensual media, with systems in place to ensure the victim’s privacy is protected.

* Social Media Platforms: Social media can be a powerful tool for perpetrators, enhancing monitoring and control. Platforms should:

  - Comprehensive Blocking Systems: Provide blocking systems that go beyond individual accounts, potentially linking accounts and devices associated with a blocked user to prevent continued harassment or monitoring.

  - Restricted Messaging: Enable users to set privacy controls that allow only approved contacts to send messages to their accounts.

* Browser and Search Data: Browsers and search engines should prioritize privacy and security:

  - Automatic Deletion: Browser history, search information, and related metadata should be deleted by default after each session or within a specified time frame (triggered by users, for example). This protects users from unwanted surveillance.

* End-to-end encryption must be the default for any messaging in order to prevent network monitoring and ensure that digital communications remain private.

* Gender Sensitivity in Design:

  - Gender-Informed Design: Designers should adopt a gender-sensitive approach when developing tools and applications. Recognizing the structural inequalities inherent in IPV helps build systems that are supportive of the unique needs of victims.

* Local Attackers and Sensitive Applications

  - Security for Local Attackers: When designing sensitive applications, ensure that they are secure against local attackers, including those who may have physical access to the device. Sensitive applications refer to any software or services that handle private or confidential data, such as personal accounts, financial tools, and communication platforms.

* Detection Tools and Analytics

- Building Detection Tools: Develop advanced detection tools with IPV-specific algorithms and systems. These tools should focus on identifying patterns of control and abuse, as well as enhancing logging and analytics for detecting unusual or suspicious activity. Consider guidance for building such tools [UNGUI].

* Engineer plausible deniability for sensitive applications.

* Build detection tools and improve logging and analytics for user agents and devices with IPV in mind.

* Transparent Reporting: IPV-related issues should not be viewed solely as privacy concerns. It’ s crucial to address areas such as transparency in reporting mechanisms, identity management, and proper accountability measures in tech systems to counter the misuse of power.

It is important to note that IPV should not be mistaken to be a privacy issue alone. Furthermore any tech-based solutions and interventions that only address privacy can be used by attackers, helping them to cloak their attacks from the victim and other means of detection. Power is imbalanced in IPV and technology entrenches power.[Citron]

It’s essential to acknowledge as well that implementing these recommendations will not fully eliminate IPV due to the broader power imbalances in society. However, these measures can play a critical role in addressing the use of technology to facilitate abuse. Addressing IPV through technology must be viewed as a step toward giving victims the tools to regain control, while simultaneously limiting the means by which abusers can continue their attacks.

6. Resources

* Cornell Tech’s Clinic to End Tech Abuse
  https://www.ceta.tech.cornell.edu/

* List of domestic violence hotlines around the world
  https://en.wikipedia.org/wiki/List_of_domestic_violence_hotlines

* Procedures and tools for clinical computer security
  https://www.usenix.org/conference/usenixsecurity19/presentation/havron

7. Security Considerations

This document itself discusses security threats in the context of IPV. Implementers should note that mitigation mechanisms must balance user safety, usability, and privacy. In particular, features intended to protect users (e.g., encryption, logging, blocking) can also be exploited by abusers if not designed with IPV contexts in mind.

8. IANA Considerations

This document has no actions for IANA.

9. Informative References

[APCFramework]
Communication, A. for P., "A framework for developing gender-reponsive cybersecurity policy", n.d., <https://www.apc.org/sites/default/files/gender-cybersecurity-policy-litreview.pdf>.

[CDOHPFLDMR]
Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., Levy, K., Dell, N., McCoy, D., Ristenpart, T., and E. Tseng, "The Spyware Used in Intimate Partner Violence", n.d., <https://ieeexplore.ieee.org/document/8418618>.

[CETAStrategies]
Abuse, C. to E. T., "Resources from the Clinic to End Tech Abuse", n.d., <https://www.ceta.tech.cornell.edu/resources>.

[Citron] Citron, D. K., "The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age", 2023, <https://wwnorton.com/books/9780393882315>.

[CSP] Abuse, C. to E. T., "Computer Security and Privacy for Survivors of Intimate Partner Violence", n.d., <https://www.ipvtechresearch.org>.

[Dragiewicz2018]
Dragiewicz, M., Burgess, J., Matamoros-Fernndez, A., Salter, M., Suzor, N. P., Woodlock, D., and B. Harris, "Technology facilitated coercive control: domestic violence and the competing roles of digital media platforms", 6 September 2022, <https://www.tandfonline.com/doi/abs/10.1080/14680777.2018.1447341>.

[DULT] WG, I. D., "Detecting Unwanted Location Trackers", n.d., <https://datatracker.ietf.org/wg/dult/about/>.

[Freed] Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., and N. Dell, "Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders", 2017, <https://doi.org/10.1145/3134681>.

[IPVTechBib]
Maynier, E., "Selected Research Papers on Technology used in Intimate Partner Violence", n.d., <https://ipvtechbib.randhome.io/>.

[NCAV] Abuse, N. C. A. D. V., "National Statistics Domestic Violence", 6 September 2022, <https://ncadv.org/learn-more/statistics>.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <https://www.rfc-editor.org/rfc/rfc6973>.

[RFC7624] Barnes, R., Schneier, B., Jennings, C., Hardie, T., Trammell, B., Huitema, C., and D. Borkmann, "Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement", RFC 7624, DOI 10.17487/RFC7624, August 2015, <https://www.rfc-editor.org/rfc/rfc7624>.

[TBMDGMMDR]
Tseng, E., Bellini, R., McDonald, N., Danos, M., Greenstadt, R., McCoy, D., Dell, N., and T. Ristenpart, "The Tools and Tactics Used in Intimate Partner Surveillance: An Analysis of Online Infidelity Forums", n.d., <https://arxiv.org/abs/2005.14341>.

[UNGUI] Division, U. N. P. F. G. T., "Guidance on safe and ethical use of technology to address GBV and HP", n.d., <https://datatracker.ietf.org/meeting/118/materials/slides-118-hrpc-unfpa-gbv-tech-guidance-00>.

[UPMSG] Unbreakable, "Unbreakable: Designing for Trustworthiness in Private Messaging", n.d., <https://www.designtrustworthymessaging.org/>.

[WHO] Organization, W. H., "Understanding and Addressing Violence Against Women: Intimate Partner Violence", 2012, <https://apps.who.int/iris/bitstream/handle/10665/77432/WHO_RHR_12.36_eng.pdf>.

[Witness] Gregory, S., "Deepfakes, misinformation and disinformation and authenticity infrastructure responses: Impacts on frontline witnessing, distant witnessing, and civic journalism", n.d., <https://journals.sagepub.com/doi/10.1177/14648849211060644>.

Acknowledgments

Thanks to:

* Lana Ramjit and Thomas Ristenpart for their inspiring work on this area, and guidance for this draft.

* Shivan Kaul and Pete Snyder for discussions, guidance and support.

Authors' Addresses

Sofia Celi
Brave
Email: cherenkov@riseup.net

Juliana Guerra
Email: juliana@usuarix.net

Mallory Knodel
CDT
Email: mknodel@cdt.org