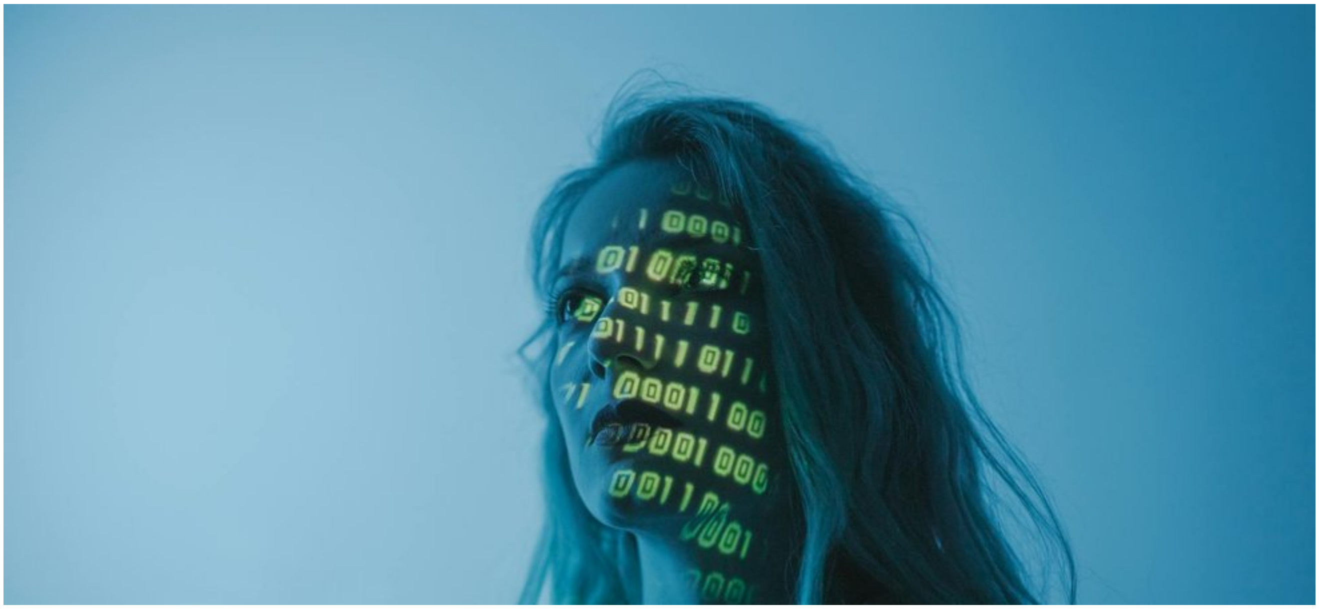
NEW AMERICA



November 2024

Gendered Harms of Data Weaponization

Historical Patterns, New Battlefields, and the Implications for Democracy and National Security

Pavlina Pavlova

Future Security
Last edited on November 14, 2024 at 9:35 a.m. EST

Acknowledgments

A special acknowledgement to Lauren Zabierek, Camille Stewart Gloster, Lauren Buitta, James Shires, Bridget Chan, and others who contributed their time to inform and shape the ideas presented here.

Editorial disclosure: The views expressed in this report are solely those of the author(s) and do not reflect the views of New America, its staff, fellows, funders, or board of directors.

About the Author

Pavlina Pavlova is a 2024 #ShareTheMicInCyber Fellow.

About New America

We are dedicated to renewing the promise of America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Future Security

Future Security is a partnership between New America and Arizona State University. It reconceptualizes U.S. security policy towards a holistic engagement with current and future challenges including domestic terrorism, armed drones, climate change, pandemics, rising authoritarianism, and new and emerging technologies.

About #ShareTheMicInCyber Fellowship

The #STMIC Fellowship, hosted in partnership between #ShareTheMicInCyber and New America, is designed to advance diversity and inclusion in cybersecurity field.

Contents

Contents Cont'd

Executive Summary

Data weaponization has emerged as a key instrument in the toolbox of malicious actors and individuals who exploit sensitive information and intimate images to harm their targets. The intersection of data and gender leads to serious consequences that perpetuate inequality, undermine security, and restrict access to essential services.

The research follows four factors—data, control, perception, and access—that explain why and how certain types of data weaponization inflict gender-specific harm. The observed cascading and compounding dynamics demonstrate how one form of gendered harm can trigger another, aggravating the overall negative impacts. As a result, victims can become trapped in a cycle of harm, where the initial harm leads to deeper and more acute harms. The analysis across all four factors highlight the following themes:

- **Gendered harm is both contextual and intersectional.** The context is formed by policy and legal frameworks, gender norms and roles imposed by society and the state, access to services, social and family structures, and the environment. Victims' gender and intersecting identities, such as sexuality, race, employment, and visibility, further influence the type, likelihood, and intensity of harm.

- **The online and offline dimensions of gendered harm are deeply interconnected.** Although data exploitation occurs in the digital realm, it intersects with offline events and experiences. The far-reaching repercussions extend into both spheres**,** reinforcing each other. This interconnectedness underscores the pervasive nature of gendered harm.

- **Harm from data weaponization poses critical challenges to democracy and national security.** The increasing frequency, scale, and impact threaten individual rights and exacerbate broader security risks. Attacks that exploit gender can hinder participation of women and gender and sexual minorities in public life, eventuating into a democratic deficit. Such exploitation can also lead to discriminatory access to services and mistrust in platforms, further excluding targeted groups and individuals from engaging in society on equal footing.

Current policies and legal frameworks fail to effectively address the gendered dimensions of data weaponization. Cumbersome legal responses to rapidly evolving tactics, lack of state capacity to address harmful practices, and insufficient victim support mechanisms contribute to the underreporting and under-addressing of gender-specific harms. Existing frameworks often overlook the intersectional impacts of data breaches and multiple data exploitations,

limiting the effectiveness of policy and technology responses. The absence of disaggregated data and established methodologies further hinders the documentation, quantification, and qualification of gendered harm, obstructing to identify and substantiate aggregate trends.

Introduction

Data weaponization has emerged as a main threat in the current cyber landscape. Any sector that is the custodian of sensitive data, including those providing critical services such as health care, can be targeted or affected by data breaches, ransom demands, and subsequent disruption of services. Similarly, online applications that collect personal information, and which business model supports intrusive data collection, such as dating websites, femtech, and smart devices, risk having user information accessed and shared by third parties. Data weaponization often does not stop there. Once acquired, information and content can be employed to manipulate, deceive, coerce, or attack victims—entrapping individuals in a cycle of harm. As perpetrators aim to maximize inflicted damage, the pressure on the targets is immense.

Different groups interact with and relate to technology in diverse ways, and not everyone is impacted equally. Identity shapes perceptions, roles, and access and can be a parameter amplifying the risk of abuse and violence. Gender and sexual preference in particular can impact and even determine the nature and severity of harm. For women and LGBTQ people, data weaponization can exacerbate existing vulnerabilities and create new ones, leading to more severe, prolonged, and far-reaching consequences. Several gendered cyber harms have been acknowledged, including, but not limited to, a disproportionate impact of technology-enabled gender-based violence on women, cyberstalking, online harassment, nonconsensual dissemination of information, as well as disinformation and data breaches. However, the interplay between various types of data-exploiting attacks and their unique risks to individuals based on gender remains underexplored.

This paper examines the critical intersection of data weaponization and gender, evidencing the disproportionate and often devastating impacts it inflicts on the victims. The research is organized around four factors: data, control, perception, and access. Each of these factors can lead to gendered harm, while they often intersect and interact in real life. The limitations of this research pertain to the paper exclusively focusing on the experiences of women. Considerations for LGBTQ individuals are included when the nature of the harm or the type of attack is similar or comparable to those experienced by women. Intersectional identities such as gender expression, race, socioeconomic status, ethnicity, and health status, while considered, are not explored in further detail. The research acknowledges that both men and women can experience harm due to distinct vulnerabilities, but the analysis does not extend to considerations for male victims. Further qualitative research, victim testimonies, and quantitative data are needed to evidence how data exploitation impacts people differently based on gender, intersectional identities, and other contextual attributes.

Data Weaponization and Gender

Data weaponization is the act of using data to manipulate, deceive, coerce, or attack someone or otherwise inflict harm. Data can be acquired and misused in various ways, depending on whether it is publicly available or restricted, and if restricted, whether access is authorized or unauthorized. For instance, data breach occurs when restricted data is accessed without authorization by external perpetrators. It can also be leaked through unauthorized disclosure when individuals disclose data either accidentally or with malicious intent. If access to data is authorized, the authorization may be granted knowingly or under false pretenses, such as through social engineering techniques and other forms of manipulation. Additionally, data can be extracted by coercing and intimidating the targets.

"Data weaponization is the act of using data to manipulate, deceive, coerce, or attack someone or otherwise inflict harm."

In cases when data is given knowingly, using it beyond the scope of authorization in terms of time or function can constitute data weaponization. This occurs as a result of excessive data collection and sharing practices, where data is utilized for unauthorized purposes without the user's consent.[1] Publicly available data can be misused for malicious purposes, including, doxing, stalking, and other forms of harassment. Additionally, audio and image data that is publicly accessible can be manipulated or employed in synthetic media to create deepfakes.

Not all data is equally susceptible to misuse. Personal and sensitive data poses the highest risks of exploitation. Personal data comprises name, address, phone number, email, and biometrics, while sensitive data includes medical information and data related to gender identity or sexual history and orientation. A combination of personal and sensitive data is typically more high-risk than a single piece of personal information.[2] For example, data breaches involving medical data can cause more harm if they are combined with personally identifiable information.[3]

Harm can be defined as direct and/or indirect, immediate and/or long-term adverse effects of an attack on the victim. Serious harm occurs where the harm arising from an attack has resulted, or may result, in a real and substantial detrimental effect on the individual. That is, the effect on the individual is more than mere irritation, annoyance, or inconvenience. Harm to an individual includes physical harm; economic, financial or material harm; emotional or psychological harm; and reputational harm. A person may be impacted by one type or a combination of different forms of harm.[4] The gravity of harm depends on the consequences experienced by the victim, such as irreversibility, duration of exposure, and extent of damage.[5] Both identity and context influence the nature and severity of inflicted harm, and vary based on the type of personal information exposed, the level of sensitivity of the data, the duration for which the information was accessible, as well as personal circumstances, including vulnerability or susceptibility to harm. Contextual aspects encompass the various circumstances, conditions, and environment in which the attack occurred, and the actions taken to prevent and mitigate the harm.

Gendered harms refer to adverse effects to a person based on—and often specific or exclusive to—their gender. These are often negative impacts, including those that reinforce existing gender norms, biases, stereotypes, discrimination, power structures, and other harmful dynamics.[6] While this paper assesses gender in terms of vulnerability, women as well as gender and sexual minorities are not inherently vulnerable groups, meaning they are not vulnerable by nature and in all times and places. Perceiving them primarily as victims can exacerbate gender stereotypes and bias, lead to unintended negative consequences, and distract from the actual structural and systemic causes of gendered harm.[7]

“Gendered harms refer to adverse effects to a person based on—and often specific or exclusive to—their gender.”

Gender can be defined as the attributes and opportunities associated with being male and female. While definitions of gender vary, it is commonly understood that gender exists on a spectrum and is socio-culturally constructed. The word “gender” is not synonymous or interchangeable with “women.”[8] Gender norms are changeable over time; they inform individual identities, social relations, and the distribution of resources and power in society. Although gender is often comprehended as expressing expectations regarding appropriate behavior for men and women, gender is nonbinary and diverse. It refers to people of all gender identities and expressions. Gender equality therefore refers to equal rights, opportunities, and outcomes for men, women, girls, boys, and people of diverse gender identities and expressions. Gender identity is the deeply felt understanding of one’s gender.[9]

Four Factors of Gendered Harms

To evidence gender as a point of vulnerability impacting and even determining the nature and severity of harms caused by data weaponization, this research proposes four categories or "factors": data, control, perception, and access. These categories help to capture the gender-specific aspect of various attacks. Importantly, the factors interact, cascade, and compound, as observed in a Chatham House report: "[Gendered harms] are cascading because one form of gendered cyber harm leads to another. They are compounding because such cascades increase the impact on the people affected."[10] The intersection of these factors reinforces the gender dimension of data weaponization and the severity of experienced harm.

Data breaches and unauthorized disclosure of gender-specific **data**, such as information about reproductive health, gender identity or sexual preference, can result in gendered harms. Weaponization of medical data through hack-and-leak operations, ransomware attacks, and multiple extortions may inflict reputational, psychological, and legal harms on victims. The commodification of sensitive data from fertility apps, or "femtech," and dating apps fuels abuse by enabling unauthorized sharing of intimate information, including those relating to abortions and HIV status, leading to exploitation, stigma, and discrimination, especially in societies where such behavior is criminalized or stigmatized.

"Data can be weaponized to exert control over individuals and communities...These dynamics can be present both in intimate relationships or as part of broader societal power imbalances."

Data can be weaponized to exert **control** over individuals and communities based on existing gender dynamics. These dynamics can be present both in intimate relationships—in the form of domestic violence, especially intimate-partner violence—or as part of broader societal power imbalances manifested in patriarchal systems. In such contexts, even personal data that is not gender-specific, such as addresses, contact information, or communication metadata, can be weaponized in a gendered way to facilitate stalking, surveillance, harassment, and violence.

Perception is inherently gendered, as women's sexuality and agency have been viewed differently and measured against different standards than men's. Similarly, LGBTQ individuals have faced distinct and discriminatory perceptions. This factor helps to capture how sexist, misogynistic, biased, and discriminatory attitudes fuel data weaponization to humiliate, defame, or destroy reputations. Examples include cases when data and images are fed into defamation and disinformation campaigns, or used in nonconsensual sharing of intimate images.

Access to essential services can increase gendered harms when data weaponization leads to operational disruption or otherwise limits the availability of facilities, assistance, or information related to gender-specific care, such as those provided by abortion clinics and transgender centers. Gendered harms also emerge when the operational disruption impacts vital services that women and queer individuals rely on and already face barriers to access. In addition, considering the traditional gender roles and social norms regarding caregiving responsibilities and unpaid domestic labor that are still prevalent in certain settings, women may be further disproportionately impacted by attacks against a range of critical infrastructure sectors, including health care, education, and transportation.

1. The Data Factor

Health Care Data

The protection and confidentiality of sensitive data are essential to safeguarding an individual's privacy, personal security, and fundamental human rights, and ensures their ability to exercise autonomy and agency. Data breaches can have severe repercussions for the affected people, and their gendered impacts can be evidenced in the attacks on health care data and information leaks about gender and sexual identity. When gender-specific data is accessed, even in the case of indiscriminate attacks that do not target specific individuals or groups, such incidents can have a distinct and disproportionate impact on women and LGBTQ people. Breaches of medical data related to sexual and reproductive health, including details of pregnancy stages and cases of abortion, can affect not only women's privacy but also their health, dignity, self-development, societal and psychological well-being, physical security, and access to services. The negative consequences are pronounced in countries where abortion is illegal or in traditional and patriarchal societies, where women and medical practitioners face serious repercussions. Similarly, data leaks can put people of diverse gender identities, expressions, and sexualities at risk of being involuntarily outed. Exposing their identity and sexual preference can lead to family rejection, societal ostracization, and loss of employment.[11] Moreover, given the precarious nature of the positioning of LGBTQ communities in society and how vulnerable these individuals are to mental and physical abuse, data breaches can expose victims to further stigmatization and violence. [12]

Attacks on the health care sector have intensified, leaving millions of patients affected by data breaches.[13] These attacks have a gendered dimension if gender-specific data is leaked, when gender is weaponized to exacerbate harm, or when attacks have a gendered motivation in the first place. Even if there is no immediate evidence of the data resurfacing on the dark web or misused for ransom demands, once data is hacked, there is no reassurance it will not be eventually leaked. At the same time, breaches of sensitive medical data can erode trust in health care services, leading to long-lasting harm. In June 2024, the Russia-speaking Qilin Ransomware-as-a-Service (RaaS) group, also known as Agenda, attacked blood matching tests for several health care organizations operating as part of the National Health Service in London. Breached sensitive data, including the results of blood tests for HIV, were published online by the cybercriminal group on a messaging platform.[14] In May 2023, a ransomware attack by Russian-speaking RaaS group TA505, known as Clop, targeted the Better Outcomes Registry & Network, a perinatal and child registry in Ontario, Canada. The incident, caused by vulnerabilities in the MOVEit file transfer service, led to a data breach.[15] The ripple effect impacted hospitals, midwife practices, fertility clinics, and neonatal intensive care units and compromised personal information of 3.4 million people seeking pregnancy care between 2010 and 2023. Data of mothers, newborn babies, and parents seeking fertility treatment were exposed, including names, home addresses, and health card numbers, along with lab test results, procedures, and outcomes relating to pregnancy and newborn care.[16] The combination of personal data and medical data aggravated the potential harm.[17]

A knowledge gap remains regarding the full spectrum of consequences resulting from data breaches.[18] Accounts of victims' personal experience remain anecdotal and captured in individual testimonies. For instance, in October 2023, a data breach at a Melbourne hospital led to unauthorized access to medical data of more than 190 patients treated there. A patient whose details were exposed shared that she had been affected by other data breaches, but this one has been the most difficult for her, because "they [the targeted organization] were able to confirm at this stage what information [of the patient] has appeared on the dark web, but they said there is no guarantee that it will not appear in the future. My health records are safe in the hospital vault essentially, but a lot of the other details have been leaked."[19] Once a data breach occurs, the compromised data may be carelessly stored by actors with little concern for maintaining its privacy. This highlights the permanence of harm that follows once data is accessed.

Victims of data breaches can experience psychological insecurity, violation, and trauma. They can also face criminal charges in countries where abortion is illegal. In July 2016, due to a security failure, a database of the Municipality of São Paulo in Brazil was published, exposing personal and medical data of an estimated 650,000 patients, including public agents from the public health system. The medical data comprised sensitive gender-specific information such as pregnancy stages and abortions. There have not been reported cases of women being charged in the outcome of this incident, but the data breach raised serious concerns about the potential for legal repercussions in a country where abortion is heavily restricted and often criminalized with no exceptions for birth defects.[20]

Not only have attacks on health care become more common—patient data breaches doubled in 2023—hackers have also refined strategies to exacerbate harm.[21] As organizations have learnt to retrieve customer data through backups, hackers have become more aggressive, leaking the stolen data on the dark web and online platforms and coercing the target organizations and victims through multiple extortions.[22] An illustrative case was disclosed in February 2023, when a Russian-speaking RaaS group ALPHV, known as BlackCat, attempted to extort a health care network in Pennsylvania by publishing photographs of breast cancer patients.[23] Data weaponization can inflict reputational damage and victimize women for their reproductive health choices. In a ransomware attack against the Australian health insurer Medibank in October 2022, cybercriminals accessed records of almost 10 million customers. The Russian-speaking RaaS group REvil, also known as Sodinokibi, leaked sensitive medical data on the dark web, including a spreadsheet listing 303 patients alongside billing codes related to pregnancy terminations, such as nonviable pregnancies, miscarriages, and ectopic pregnancies. The dataset sorted patients into "good" and "bad" lists based on the trimester during the abortion occurred.[24]

Gender can also serve as the primary motivation behind attacks. In a 2012 case, a member of the hacking collective Anonymous breached the website of Britain's largest abortion provider with the intent to release the personal details of women who had used its services. The perpetrator stole around 10,000 database records containing the personal details of women registered on the British Pregnancy Advisory Service site. This case highlights how the stigma surrounding abortions can lead to women being disproportionately impacted and deliberately targeted by data breaches. The perpetrator confessed being motivated by his disagreement with his two friends' abortion, the presiding judge describing the attacker as a "zealot with an anti-abortion campaign."[25]

LGBTQ communities face increased risks concerning the privacy of medical data and information related to gender identity and sexual orientation. In February 2019, the medical records of 14,200 people living with HIV in Singapore were published online, exposing them to significant harm.[26] The perpetrator, the partner of a Singaporean doctor with authorized access to the database, gained unauthorized access to confidential information from the country's HIV registry. He then threatened to release sensitive and personalized medical data unless his husband was released from prison and the database was shut down. The medical data included information about LGBTQ individuals, many of whom had not publicly disclosed their HIV status, leaving them vulnerable to stigma and discrimination. This risk was especially significant in a country where sexual activity between men was criminalized until 2007 and only fully legalized in 2022. The perpetrator, a U.S. citizen, pleaded not guilty, claiming that his actions were intended to highlight security lapses in the database, which he argued was discriminatory. His partner, a Singaporean doctor, was charged under Singapore's Official Secrets Act for failing to safeguard the information.[27] Following the incident, LGBTQ rights organizations warned of an increase in hateful comments and heightened stigmatization of individuals living with HIV. [29]

Data-Sharing with Third Parties

Medical data can be given knowingly, but used for unauthorized purposes, undermining the principle of purpose limitation in responsible processing of personal data. Data sharing with third parties without informed consent, as well as excessive data collection and data sharing practices, constitutes data weaponization. The gendered dimension is pronounced in femtech, such as fertility apps, which collect information on menstrual cycles, sexual activity, opportunities for conceiving a child, and symptoms and stages of pregnancy. Femtech engages in widespread data misuse.[29] According to the Organization for the Review of Care and Health Apps, most period trackers share data with third parties.[30] Research by Mozilla, examining over 20 pregnancy and period tracking apps for privacy and security features, concluded that the majority of analyzed apps collected large amounts of personal data and shared it with third parties.[31] Capitalization of reproductive health has become a common business model facilitated in and through technology at the expense of women.[32]

The extensive commodification of sensitive data by femtech constitutes gendered harm. This data is vulnerable to breaches, leaks, commercial de-anonymization, publication, and exploitation. Unauthorized sharing of personal information related to sexual and reproductive health can inflict harms ranging from psychological, such as the distress caused by inappropriate fertility advertising targeting miscarriage victims, to physical and legal harms for individuals seeking abortions. App providers may be requested to share this data with the authorities in places where abortions are illegal or where abortion and reproductive health care are limited.[33] The Centre for Feminist Foreign Policy highlights that without privacy standards in place to protect user personal and medical information, women are largely on their own to safeguard sensitive health data that companies routinely collect.[34]

Since the U.S. Supreme Court's decision to overturn *Roe v. Wade*, privacy advocates have urged women to delete period tracking apps, citing concerns that fertility data could be used against the users.[35] In addition to gender-specific femtech data, information about accessing online health services, combined with location data indicating proximity to sexual and reproductive health facilities, may be monitored by law enforcement to track and prosecute individuals seeking abortion.[36] To support these concerns, the Surveillance Technology Oversight Project released a report explaining how anti-abortion governments and private entities surveil women's search history, location data, and social media content.[37] As a result, privacy violations in femtech, coupled with surveillance practices, contribute to the broader erosion and stigmatization of women's reproductive rights and can interfere with their rights to access medical information and services.[38]

Dating Platforms

Dating platforms that collect sensitive data raise privacy and security concerns. If a dating app catering to queer individuals suffers a data breach, the exposure can expose users' gender identity and sexual orientation without their consent. Since activities related to gender expression and sexuality are frequently stigmatized and even criminalized, the repercussions of such incidents can be severe, with victims finding it nearly impossible to seek justice or recourse. In November 2021, cybercriminals hacked and leaked data from the LGBTQ dating site "Atraf," revealing sensitive information such as sexual orientation and HIV status. The Israeli platform, which primarily serves male clients, left many fearing that personal data could be exposed, with some victims describing the breach as life-threatening. The tactics, techniques, and procedures used, including methods of victim-blaming to coerce ransom payments, led to allegations that the incident was linked to the Iranian-affiliated threat actor Black Shadow. [39]

The overzealous data collection by dating and social apps is accompanied by weak privacy practices. Mozilla's 2024 review of dating apps found that unless users actively opt out, dating websites could be selling their personal data for profit. The report continues to suggest that the privacy practices of dating apps have worsened since the initial review in 2021.[40] Recorded Future research into threat activity targeting popular LGBTQ social apps concluded that these apps can be targeted by actors on the dark web and in underground markets and forums. Across the five chosen social apps analyzed by Recorded Future, 77 percent of the targeted activity is listings for the sale of compromised account credentials and associated user data on dark web markets.[41] This is alarming, especially in regard to the combination of gender-specific data and location data that such applications collect and share.

The LGBTQ community is extremely vulnerable when access to sensitive data intersects with state control, such as when dating apps are used by authorities to target individuals.[42] For example, Egypt has a long history of prosecuting queer individuals. Domestic law does not directly prohibit "homosexuality," but a complex legal structure of interpretations and precedents facilitates continuous and targeted persecution of queer individuals. Egyptian prosecutors increasingly rely on digital evidence to prosecute people through online dating app entrapments. Queer activists and groups in Egypt warned members of the LGBTQ community to refrain from using apps with built-in location tracking or social media that can be monitored.[43]

A 2018 report by Article 19 detailed how dating apps have been weaponized to enable blackmail and arrests in Egypt, Lebanon, and Iran. The investigation revealed that cybercriminals, offenders, and even law enforcement use these platforms to entrap individuals, luring them into offline meetings through "catfishing" or coercing them into sharing sensitive information and intimate images.[44] Despite numerous instances of abuse, dating apps continue to operate, using a dangerous combination of courting at-risk users and failing to protect their privacy and security. For example, Grindr, a widely used app, particularly in the Arab world, was found to have sold users' location data for years through ad networks, potentially exposing the movements, work locations, and home addresses of millions of gay men.[45] The revelation followed years of Grindr's data privacy failures, including allowing anyone to pinpoint users with a triangulation technique.[46] Given the vulnerable position of gender and sexual minorities in society and how vulnerable they are to abuse, these exploitative data practices inflict severe gendered harm.

2. The Control Factor

Data Breaches Enabling Gender-Based Violence

Data can be weaponized to exert control over individuals, often reinforcing existing gender dynamics and vulnerability. Breaches of personal data such as names, numbers, addresses, or employers, while themselves not gender-specific, can inflict gendered harms and put women at higher risk of doxing, stalking, surveillance, harassment, sexual violence, intimidation, and physical abuse.[47] For example, in a 2018 case, several women had been contacted following breaches of personal information at Crosshouse Hospital. The affected individuals were notified that their personal information, including phone numbers and addresses, had been accessed by a staff member who had "no legitimate clinical or administrative requirement." The perpetrator was charged in connection with stalking and data protection offenses.[48] Data breaches can result in increased risks of harassment or intimidation to which individuals impacted by domestic violence may be more susceptible. Personal data of at-risk persons accessed by ex-partners or other untoward persons can be misused and eventuate into psychological or physical harm.[49] In March 2022, the Wakefield Council in the United Kingdom was handling child protection court proceedings when it sent documents, including the address, where the victim lived with her children, to the abuser. As a result of the data breach, the domestic violence victim and her children had to be urgently rehoused.[50]

Indiscriminate leaks of location and contact information also impact women differently, and more severely, when considering the prevalence of gender-based violence.[51] According to the figures published by the UNODC, some 47,000 women and girls worldwide were killed by their intimate partners or other family members in 2020, with many more leaving their homes to seek safety from domestic abuse.[52] These numbers are alarming, especially considering that breaches of personally identifiable data become increasingly common each year. To illustrate the gendered harms that can arise from personal data leaks, consider the case in July 2016 when WikiLeaks published extensive databases exposing the personal information of 50 million Turkish citizens, including a near-comprehensive database of adult women in the country. Although the hackers were not targeting women specifically, the attack had a disproportionate effect on women. Their addresses became available to stalkers, ex-partners, or disapproving relatives in a country recording high numbers of gender-based violence.[53]

In January 2018, the data breach of the Aadhaar database, the world's largest biometric ID system, exposed the personal and biometric information of over a billion Indian citizens. The compromised data included names, addresses, photos, phone numbers, emails, and biometric information. The website's application programming interface, which did not have required access controls, was connected to the Aadhaar database. Hackers exploited this vulnerability and sold access to the personal data via a WhatsApp group.[54] Similar concerns arose from the AT&T hack in April 2024, when hackers compromised six months' worth of call and text message records for nearly all AT&T cellular network customers, exposing sensitive metadata related to their communications. The content of the calls and messages was not compromised, and customers' personal information was not accessed, but the records included phone numbers. Metadata revealing information about communications is highly sensitive, especially when collected and analyzed at large scales to reveal patterns of behavior and connections between people.[55]

Surveillance Apps and the Internet of Things

Men have been found to be more likely to commit cybercrimes, especially those associated with hacking and gender-based offenses, such as using spyware against intimate partners and sharing nonconsensual intimate images online. At the same time, women are particularly vulnerable to digital surveillance and control committed by partners or family members as a form of surveillance, control, and continuing the cycle of family or intimate partner abuse.[56] Though intimate partner violence impacts all genders, women comprise the majority of victims in heterosexual relationships. A 2023 Australian study further indicates that the prevalence of technology-facilitated abuse might be higher in sexual and gender minority relationships than in heteronormative ones.[57]

To gain access to their targets' private data, attackers can use surveillance applications known as "stalkerware" or "spouseware," which enable unauthorized individuals to covertly monitor the digital activities of others. An entire industry dedicated to developing digital surveillance tools operates largely unregulated, driven by commercial demand. Monitoring software can be installed in secrecy through dual-use apps and masked by socially accepted labels such as "parental control."[58] Consumer mobile spyware apps are able to monitor user activity, including text messages, phone calls, and location, and transmit the information to the abuser. The perception of threat alone can cause significant harm to victims, as the mere awareness of a pervasive danger serves as a form of control.[59] The Coalition Against Stalkerware reported a significant spike in the use of the surveillance software during the coronavirus pandemic, with a 780 percent increase in detections of monitoring apps. This rise correlates with increased domestic violence reports, as many individuals were confined to their homes and reliant on technology for communication.[60] An Access Now report highlights that the use of stalkerware can have a "devastating impact on women targets, especially given the lack of robust legal or social protections against gender-based violence—which includes physical, economic, mental, and other harms—and the many hurdles presented by existing political, societal, and gender power asymmetries."[61]

The Internet of Things (IoT) devices provide further vectors for exerting control. Attackers can repurpose dual-use applications built for beneficial or innocuous purposes. For example, anti-theft devices such as doorbell cameras can be used for stalking.[62] Devices like fitness trackers and item-finding software can also facilitate abusive practices.[63] The Department of Computer Science of the University College London conducted research evidencing that technology-facilitated abuse flourishes through unauthorized use of phones, trackers, and other emerging technology, changing the nature of intimate partner violence.[64] Dual-use devices and applications can extend the sense of the perpetrator's presence, further isolating, punishing, or humiliating victims and preventing them from seeking and receiving support.[65] Nearly any system that collects and shares location data can be weaponized against its users. This includes vehicles that gather extensive information about drivers, including their location and driving patterns.[66] A report by the International Digital Accountability Council further uncovered that some of these devices and apps sent unencrypted personal information to third parties.[67] Data weaponization in its gendered form poses a significant public health issue, affecting the target's mental and physical health, dignity, self-development, and access to services.[68]

Abuse of Spyware and Data Collection by States

The frequency and prevalence of violence against women and gender and sexual minorities are linked to patriarchal systems of government that politicize gender and exert control over nonconforming citizens.[69] By allowing gender-based violence in public life, and not providing recourse for victims, states normalize abusive practices. In this way, gender plays a key role both as a social structure and a system of power. In this context, collecting private data about the locations, contacts, and activities of women and queer individuals is often part of a broader strategy aimed at surveilling, harassing, intimidating, and ultimately silencing targeted groups. The use of surveillance software for these purposes can inflict gendered harms, isolating victims and threatening to expose their contacts or intimate lives. This type of data weaponization is extremely harmful to LGBTQ individuals and advocates. For example, according to a *Haaretz* investigation in 2018, the Indonesian government purchased surveillance software to create a database of LGBTQ rights activists who had been targeted for surveillance.[70] Similar to technology-facilitated intimate partner abuse, the mere presence—or even the perceived presence—of surveillance can result in psychological harm, privacy and security concerns, and a chilling effect. This often leads targets to withdraw from social or public life or alter their behavior to conform to imposed norms. Victims of intrusive surveillance report mental stress, paranoia, social isolation, and self-censorship for fear of a possible backlash.[71]

"Collecting private data about...women and queer individuals is often part of a broader strategy aimed at surveilling, harassing, intimidating, and ultimately silencing targeted groups."

Women with public profiles, such as journalists, activists, human rights defenders, political candidates, and whistleblowers, are particularly exposed to threats that instrumentalize their gender. Targeted surveillance, interception of communications, and confiscation of devices can expose especially women to continued harm, including doxing, stalking, harassment, and physical violence.[72] Data exploitation can expose the target's private information, communication, sources, and contacts, and can even harm their family members. For instance, Citizen Lab reported that Mexican investigative journalist Carmen Aristegui and her minor son were targeted, both receiving messages containing spyware exploit links.[73] If a device becomes infected with spyware or a target falls victim to a phishing attack, it can erode trust within their communities and networks, undermining their reputation, and negatively impacting their relationships and work opportunities.

The UN Special Rapporteur on the rights to freedom of opinion and expression recognized targeted digital surveillance of journalists and media workers as one of the three major contemporary threats to the safe and free practice of journalism.[74] The Committee to Protect Journalists further concluded that "gender-based violence and harassment—both online and offline—is used to intimidate and silence female journalists, posing threats to press freedom."[75] A 2021 UNESCO report on global trends in online violence against women journalists, which surveyed over 900 female-identifying journalists in 125 countries, found that 20 percent of all respondents said they had been attacked or abused offline in connection with online violence they had experienced.[76] In 2022, Access Now and Front-Line Defenders reported that governments in the MENA region and beyond were using spyware to perpetrate human rights abuses and suppress activists and journalists.[77] The Pegasus malware has been reportedly used in more than 50 countries worldwide to infect the phones of activists, journalists, and human rights defenders, amongst others.[78] Many women's rights defenders have been targeted as part of these campaigns. Access Now highlighted that the impact of surveillance on women is particularly egregious and traumatizing, as governments have weaponized personal information extracted through spyware to fuel smear campaigns, blackmail, extort, and dox the targets and encourage others to harass them as well.[79] Prominent international cases of surveillance targeted female journalists in Russia, Azerbaijan, Mexico, and Lebanon.[80]

Data breaches, especially in high-risk environments, can eventuate into threats and physical harm. For example, the personal information of hundreds of journalists who had registered to cover national events in Mexico was hacked and posted on a website in February 2024. The leaked information contained journalists' full names, their personal identity code, and a copy of a personal identification document, prompting a call by the Committee to Protect Journalists for an immediate investigation. In Mexico, which continues to be an extremely dangerous country for journalists, privacy laws compel any government agency subjected to a data breach to immediately inform the people whose information has been leaked. However, the federal government did not inform the reporters whose information was leaked until it was already widely publicized.[81] Journalists in Mexico lack social and institutional protections, making them vulnerable to threats and aggression. The Global Initiative Against Transnational Organized Crime stressed that when analyzing violence targeting journalists in Mexico, it is also important to highlight the additional layer of gender impact.[82] According to CIMAC, a Mexico-based organization that has been documenting attacks on women journalists, attacks against female journalists in Mexico have increased fivefold between 2013 and 2022. However, gender is consistently ignored despite the additional vulnerability of women in the field.[83]

Finally, mass surveillance in public spaces can intersect with gender by facilitating control over targeted groups of population. Similar to intimate partner violence enabled by smart technology, data collection in authoritarian and patriarchal societies can lead to abusive practices that inflict gendered harm. Research by Azadeh Abkari at the University of Twente reveals that Iran leverages smart technology to surveil and police women's clothing.[84] Iranian Special Police Forces, mandated to deal with insurgency, gathered data from traffic cameras and used the data to identify and penalize women who violate the country's strict Islamic dress code. By policing women in public spaces, such data-exploitative control can severely restrict women's participation in public and social life.[85] Iran is among the many governments that utilize intrusive software and smart technologies as part of their data-driven oppressive practices.[86] This abuse has significant negative impacts on victims due to the cumulative effects of three distinct factors: the type of data being collected, who has control over that data, and how it impacts the access of the affected individuals.

3. The Perception Factor

Disinformation and Defamation Campaigns

Women and LGBTQ individuals experience distinct and discriminatory views compared to men. Misogynistic and sexualized defamation, disinformation, nonconsensual sharing of intimate images, and the resulting harassment and abuse represent a distinct form of data weaponization. This weaponization exploits gender and sexuality to shame, intimidate, and deter targets from engaging in public or social life.[87] For illustration, in the summer of 2020, phones of female journalists and activists in Saudi Arabia were infected with spyware and the acquired intimate photos circulated on social media. These coordinated defamation campaigns also fabricated narratives to accompany the images to incite outrage among conservative audiences and subject the targets to public shaming. [88] Attacks that weaponize gender carry a deeply personal impact, destroying reputations and leading to prolonged harassment and abuse. These campaigns suppress democratic engagement by preventing individuals from fully expressing themselves or participating in public life on equal footing. By publicly attacking women, perpetrators send a message to the entire group they represent. When women do not have the necessary tools to participate in contemporary political life, their absence in government institutions translates into a democratic deficit.[89] Since data manipulation in the form of fake visual content is on the rise, gender identity risks being the difference between full membership and second-class citizenship in a community of political rights.[90]

Gendered data weaponization is a national security problem since gendered defamation and disinformation have been a distinct part of the foreign interference toolkit.[91] A 2022 European Parliament report on foreign interference in democratic processes "recognizes that gendered disinformation attacks and campaigns are often used as part of a broader political strategy to undermine equal participation in democratic processes, especially for women and LGBTIQ+ people" and stresses that such disinformation fuels hate, both online and offline, and threatens lives.[92] An attack on a Finnish journalist who exposed fake news operations and a troll farm in Russia shows how sensitive data can be weaponized through systematic sexualized attacks to discredit people and institutions. In 2014, Jessikka Aro saw her medical information published online after a breach into archived court files, including data showing her fine for drug use years ago. The following coordinated defamation campaign framed her as a "NATO drug dealer," undermining her reputation and the credibility of her work. The journalist was subsequently doxed after malicious actors released her home address, and was continuously the subject of defamation campaigns alleging her of being a prostitute to CIA and NATO officials. The online abuse eventuated into death and rape threats.[93] This case of multiple data exploitations shows how disinformation campaigns can use elements of facts and fiction to inflict more severe reputational damage.[94] The cumulative effect of personal data breaches, sexist defamation campaigns, and an abusive environment illustrates the cascading and compounding nature of gendered harms—where one form of abuse leads to another, ultimately intensifying the inflicted harm.

The proliferation of fake videos depicting political figures in compromising situations poses another significant threat to the openness and fairness of elections. Sexualized, doctored images and videos purportedly showing female politicians and candidates have targeted many women, including high-profile figures in Ukraine, Rwanda, Croatia, and the United Kingdom.[95] Cara Hunter, a Northern Irish politician, was a few weeks away from the national legislative elections in 2022 when she was targeted with a coordinated campaign of AI-generated deepfake video of her performing graphic sexual acts. Within days, the false clip had gone viral, and the politician was bombarded with sexual and violent messages. She later explained her belief that the campaign aimed to undermine her politically and the deepfake would haunt her for life, because "it has left a tarnished perception of me that I cannot control."[96] Italy's Prime Minister Giorgia Meloni became a target of deepfake pornographic videos in 2020 before she took office. According to an indictment, two men were allegedly involved in creating deepfake pornographic videos using her likeness, and uploading the graphic content to an American porn website.[97]

Political candidates in the country of Georgia were victims of sexualized disinformation ahead of the 2016 parliamentary elections, targeted by fake videos depicting them engaging in sexual activities. This defamation campaign had serious consequences, especially for a female politician accused of adultery based on fabricated videos, who eventually withdrew from political life. In contrast, the male candidates targeted by the campaign did not face similar repercussions. An exception was a man identified by the media as gay, which put him at significant risk in the predominantly conservative country. While further comparative research on men and women public profiles is needed, there is evidence of a gendered dimension of these attacks through the gendered and sexualized nature of the content, as well as the harassment and intimidation such campaigns trigger. A report from the Wilson Center explored the direct and indirect impacts of widespread gendered and sexualized disinformation on women in public life.[98] The researcher highlighted that online gendered abuse is "intersectional in nature, with abusers often engaging with both sex- and race-based narratives, compounding the threat for women of color." For instance, Vice President Kamala Harris has been subject to a barrage of sexists and racist attacks, including deepfakes depicting the Vice President as a sex worker circulating on online platforms.[99] The cacophony of gendered defamation and abuse flooding the comment sections of prominent figures is united in one shared purpose: to push women out of political life. Women are singled out for abuse more often, and the nature of these digital attacks is more vicious than ones directed at their male equivalents. [100]

Nonconsensual Sharing of Intimate Images, Real or Fake

Women globally face disproportionate levels of abuse for their gender.[101] The distorted perceptions and sexualization of women and their bodies is compounded by the nonconsensual mass circulation of intimate photos. Nonconsensual sharing of intimate images exploits personal content, and can be uniquely harmful if such weaponization of data takes place in patriarchal societies that exert control over women. Unauthorized sharing of intimate images has a deep impact on victims, whose reputation is tarnished by reactions characterized by patriarchal morality and victim-blaming. If nonconsensual image sharing is a method of control, the targets face barriers in reporting crimes and seeking recourse.[102] The law can be further instrumentalized to perpetuate patriarchal gender dynamics. For example, cybercrime laws may include clauses criminalizing online content that violates public decency or morals, usually defined elsewhere in states' penal codes or criminal law, and often build on unequal standards of behavior for people according to their gender.[103] When harmful gendered norms are perpetuated within legal frameworks, it creates an environment where victims are systematically marginalized; in other words, harms are compounded when gendered expectations are codified in a system of control. Instead of receiving support and redress, targets of such abuse can face legal consequences from a justice system that should protect them.

The four following cases took place in Egypt, which has a traditionally patriarchal culture. In 2022, a woman committed suicide after her husband threatened to share intimate pictures and videos online as a form of revenge.[104] Another woman committed suicide after being blackmailed by two young men who hacked her mobile phone, obtained pictures of her, altered the photos, and republished them.[105] In a different case yet another woman committed suicide after her neighbors fabricated her pictures and blackmailed her for money.[106] In May 2020, Mawada Al-Adham, a social media celebrity, was arrested for publicly posting "indecent" photos and videos of herself on social media. The photographs of Al-Adham were shared online after being leaked from one of her mobile phones, which was stolen in 2019. Al-Adham was charged with violating the country's cybercrime law and sentenced to two years in prison and a fine.[107]

"The widespread availability of these image-generating technologies, released without adequate regulatory safeguards, has amplified existing harms and raised significant concerns over the lack of legal protections, tools, and recourse for victims."

The exploitation rooted in the sexualization of women's bodies is intensifying with the rise of synthetic media, enabled by accessible consumer-level AI tools. The widespread availability of these image-generating technologies, released without adequate regulatory safeguards, has amplified existing harms and raised significant concerns over the lack of legal protections, tools, and recourse for victims. Women are violated when their personal images—real or fake—are leaked and shared on privately owned platforms, with limited recourse to remove harmful material. This is exacerbated by platform reporting systems that fail to respond effectively to victims' requests, leaving them exposed and without means to protect their privacy. Even where legislation exists, law enforcement and justice systems frequently lack the capacity, resources, and established practices to address these issues efficiently. Victims may have legal avenues, such as suing for slander, but the abuse happens fast while the legal process is slow and cumbersome. Because of the incidence and the permanence of image-based abuse, it may re-victimize the target endlessly when harmful content circulates online.

The use of deepfake technology for sexual abuse disproportionately targets women. A study on the state of deepfakes in 2023 found that 98 percent of deepfake videos online were pornographic and that 99 percent of those targeted were women or girls. Notably, 94 percent of those featured in deepfake pornography videos work in the entertainment industry.[108] A high-profile incident took place in January 2024 when AI deepfake pornographic images of Taylor Swift proliferated on social media.[109] In this case, the concerted action of her fan base drowned the images out of online space and made online platforms block searches to curb the spread of the images.[110] Online communities can be effective in surfacing, combating, and eliminating harmful content, but in many instances of online degradation of women, the pressure and burden of redress falls entirely on the victims. They are left to protect themselves and seek recourse with limited support or resources.[111]

4. The Access Factor

Gender-Specific Care

Loss or restricted access to services can amplify gendered harms, especially when data weaponization disrupts operations or limits the availability of essential facilities, assistance, and information related to gender-specific needs. For example, weaponizing data obtained through data breaches victimizes people by putting their sensitive information at risk. This further prevents them from accessing needed services. On the other hand, targeted attacks on medical facilities providing sexual and reproductive health services, transgender care, and abortion services—where systems are compromised to punish patients and staff—can deprive women and queer individuals of vital care. Restricting access to comprehensive sexual and reproductive health information undermines an individual's rights, dignity, self-development, and overall health outcomes. Gathering and publishing location data about such facilities further endangers patients and their providers, hampering access to the services. Digital surveillance of those seeking gender-specific care increases if access to this type of care is not guaranteed and protected by the state, or when states impose bans and exerts control over services.

Abortion rights and reproductive health remain a deeply controversial political issue in many countries, with recent legislative developments in the United States highlighting the fragility of access to safe and legal abortion for those who become pregnant. The overruling of *Roe v. Wade* unleashed a torrent of regulatory and punitive activity restricting previously lawful reproductive options, extending to civil actions and criminal indictments of patients, providers, and those who facilitate abortions.[112] Anti-abortion activists have for years targeted abortion and family planning facilities, hindering access to their websites, hacking provider and patient information, and using phone location data to advertise anti-abortion materials to people who visit family planning clinics.[113] In 2015, Planned Parenthood's services were hacked, along with the National Network of Abortion Funds and Abortion Care Network, when a group of hackers breached an employee database with the intention of decrypting and releasing personally identifying provider information.[114] The data breach was followed by distributed denial-of-service attacks and doxing of Planned Parenthood's employees. The attack was intended to be both punitive, by punishing health care workers who provided reproductive health care, and disruptive, by hindering women's access to health care and timely information.[115] In October 2022, another attack targeting Planned Parenthood exposed personal information of 400,000 patients. The data breach included the reproductive health care center's network and stole files with patient information such as names and insurance details along with clinical information including diagnoses and procedures.[116]

Data collecting and sharing practices, coupled with weak privacy and security protections, are a cause of concern.[117] Data brokers have offered to sell location data that include individuals' visits to abortion clinics and Planned Parenthood. Anti-abortion protest groups also used abortion clinic data to target ads at women inside the clinics, and the same data could be used to identify women who seek out-of-state abortions in violation of applicable laws in their jurisdiction. According to a 2022 *Vice* report, SafeGraph and Placer.ai are among the data brokers evidenced to sell location data of those visiting abortion clinics, with Placer.ai even offering "heat maps" of where abortion clinic visitors live, as well as their ethnicity and average income.[118] Trans health care providers face similar data weaponization. A centralized online list called the "Gender Mapping" project used the My Maps feature on Google Maps to document the locations of thousands of establishments around the world that serve trans people, including LGBTQ community centers that provide social and emotional support. With the authors' proclaimed aim of "abolishing the gender industry," the map had been gathering location data about specialized services since February 2021. Despite Google's initial request of a court order to remove it, it was not taken down from the application until September 2022, after being widely shared on social media.[119]

Gendered harms also arise when operational disruptions affect vital services that women and queer individuals rely on, especially as they already face barriers to access. Patient health outcomes can be impacted by spillover effects from disruptions in other sectors. For instance, electricity disruptions after the energy sector is targeted with data breach can lead to prolonged power outages, forcing hospitals to triage the delivery of medical procedures to reduce their energy consumption. There is compelling evidence that women's health outcomes can be impacted more severely compared to their male counterparts because of cyberattacks on critical services. Blackouts reduce the likelihood of women giving birth in hospitals, contributing to higher mortality rates, and significantly lower odds of skilled birth attendance, which can have acute consequences for women's health. Additionally, power outages increase the risk of pregnancy complications, including difficult or early delivery and gestational diabetes mellitus.[120] While gender-disaggregated data on the health outcomes of patients during power outages remains limited, any disruption of services may disproportionately impact certain populations. This type of data exploitation has damaging impacts on marginalized groups who already face discrimination within and outside the system, including people of diverse gender identities and sexual orientations.[121]

Gender Roles and Critical Infrastructure

Considering traditional gender roles and social norms, women may be further disproportionately impacted by attacks against a range of critical infrastructure, as they continue to play a disproportionate part in frontline health and social care roles and caregiving responsibilities. Following a ransomware attack on technological platforms of Sanitas, EPS in Colombia in November 2022, research by Karisma Foundation identified and evaluated the differentiated impacts on women caregivers.[122] This work shows that gender roles can play an important role in the gravity of the consequences of cyberattacks causing disruption of services. Similar considerations relate to other sectors that can intersect with gender roles, such as education and transportation sectors. For example, pandemic-caused disruptions to daycare centers and schools disproportionately affected women, shifting child care and education back to families. This increased the workload for women, who, in many societies, already bear the primary responsibility for housework and other forms of unpaid labor.[123] Changes in work-from-home policies following disruptive data breaches might similarly impact women if they enter unpaid housework and caregiving roles.[124]

When considering that educational institutions are top targets for cyberattacks, the likelihood of children sent home due to disruptions and cyberattacks increases the possibility of women also staying home. Cyberattacks impacting schools are becoming increasingly frequent and severe. According to the K–12 Cybersecurity Resource Center, over 1,300 cyber incidents involving educational organizations were publicly disclosed across the United States between 2016 and 2021.[125] Ransomware, phishing, and malware can result in significant data breaches that cause prolonged disruptions to school operations. For example, a 2023 wave of ransomware attacks against K–12 entities in the United States disrupted entire school systems, forcing schools to shut down for several days.

The impact rippled through the communities as students were unable to attend classes and parents forced to find temporary child care.[126]

Transportation is another critical infrastructure sector that women disproportionately rely on that is vulnerable to cyberattacks. Disruptions caused by ransomware or data breaches against other sectors, such as public transit systems, can have more damaging impacts on women because they are more likely to rely on public services than men. On average, women use public transportation more than men due to lower incomes, limited access to household cars, and lower driver's license acquisition rates. Women are also more likely to take on unpaid caregiving responsibilities, either for relatives, elderly parents, or children, and rely on public transport in times of emergency.[127] Different gender roles and access to services have also been evidenced in the information and communication technology, humanitarian, and development sectors.[128] As malicious actors attack critical infrastructure at growing rates, the worsening cyber landscape will likely disproportionately impact women.[129]

Findings: A Cycle of Harm

Harm Transcends Actors, Infrastructure, and Platforms

The evidence of harm in this paper transcends actors, infrastructure, and platforms, to explain why the inflicted damage is gendered in its nature and impacts. The four factors—data, control, perception, and access—illustrate how data weaponization specifically targets and harms women and LGBTQ individuals and provides categories for different types of attacks. These factors, while each by itself can eventuate into gendered harms, often intersect and interact. The cascading dynamics, meaning that one form of gendered harm leads to another, are aggravating in their impacts, and the harm inflicted on affected people is usually more severe when two or more factors are present.[130] Due to the cascading and compounding dynamics of gendered harm, victims can become trapped in a cycle of harm, where the initial harm leads to deeper, more acute harms.

Harm Is Both Contextual and Intersectional

Gendered harm is both contextual and intersectional. The context is formed by policy and legal frameworks, gender norms and roles imposed by society and the state, access to services, social and family structures, and the environment. Consequently, gendered and punitive laws, abusive and patriarchal social structures, and misogynistic, sexist, and discriminatory attitudes increase the likelihood and severity of gendered harm experienced by victims. Victims' gender and intersecting identities—such as sexuality, race, employment, and visibility—further influence the type, likelihood, and intensity of harm. Data exploitation can incur enduring and potentially perpetual harm, depending on how long the data was exposed, in which form, how it was abused, who was the perpetrator, and who was the target.

Online and Offline Harm Reinforce Each Other

The online and offline dimensions of gendered harm reinforce each other. Data weaponization may occur exclusively online, it may also occur in connection with offline events, and it almost always has repercussions that are experienced both online and offline. Gender is not a vulnerability by itself but because it is a target of discriminatory and abusive behavior, and the higher risk of harm in the online spaces flows from inequity and exclusion in the physical world. The negative impacts are extensive and nonexhaustive. They undermine the rights of affected people, hinder progress on gender equality, and contribute to abuse, violence, and insecurity.

Concerns for Democracy and National Security

Data weaponization raises critical concerns for democracy and national security. Gendered harms lead to mistrust in platforms and services, unequal participation in public spaces and democratic processes, and discriminatory provision of vital care. Women will likely experience a disproportionate amount of harm as the frequency, scale, and impact of cyberattacks continue to rise in the coming years. Many of these attacks are deployed by state-sponsored, state-affiliated, and transnational cybercriminal groups for a myriad of financial, political, and ideological reasons.[131] In this context, it is essential to integrate gender considerations into cybersecurity strategies and policies.[132]

Current Gaps

This paper identified policy, legal, implementation, accountability, evidence, support, and research gaps.

Policy and Law

Current cybercrime policy and legal frameworks fail to protect women and LGBTQ individuals, and may further exacerbate vulnerabilities through gender-blind or overly expansive provisions. Existing legal frameworks, protection measures, and redress mechanisms are frequently inadequate, lagging behind the rapid evolution of data exploitation techniques and tactics.

Implementation

Even if policy and legal frameworks are in place, obtaining justice remains difficult. Established legal precedents, practices, and attitudes of law enforcement and prosecutors can hinder the investigation and prosecution. Barriers such as discrimination against women and the LGBTQ community further complicate reporting the incidents, making it nearly impossible for some individuals to seek help. In essence, harm is inflicted rapidly, while legal remedies—if they exist—are often significantly delayed or entirely out of reach.

Accountability

Existing accountability mechanisms are ill equipped to obtain justice, especially in cases where perpetrators are state-supported cybercriminal groups, or when the state itself is the attacker. There is little accountability for the public and private entities that commercialize, mishandle, and weaponize data. This problem is aggravated by the current lack of accountability for vendors that develop and market insecure technology, leading to the lack of adequate security measures and widespread vulnerabilities exploitable by malicious actors.

Evidence

Underreporting is prevalent and coupled with insufficient capacity to evidence these attacks. Victims experience shame and embarrassment, fear reputational risk connected to publicizing the attack, lack awareness that victimization has occurred and where to report incidents, and have low confidence that law enforcement can assist them. The most vulnerable victims are often unable or unwilling to report incidents.

Support

Victims are left on their own. Notifications about how their data has been exploited and the available avenues for redress are routinely neglected. Many victims do not have the means to pursue recourse, or the knowledge where to seek assistance. Support programs offering legal assistance and counseling are often insufficient, poorly integrated, and inaccessible or nonexistent in certain countries.

Research

The intersection of gender and data weaponization is understudied, primarily due to the lack of disaggregated data, qualitative analysis, and firsthand testimonies. This gap limits the ability to conduct thorough and comparative analysis of how gender and intersecting identities shape the experiences of different groups facing data weaponization.

Recommendations

By recognizing and understanding the links between gendered harms in data weaponization, states, private actors, and civil society can more effectively prevent, counter, and mitigate these harms. This report offers a set of recommendations to achieve this.

Incorporate Gender Analysis in Policy and Law

States should **mainstream gender into policies, legal frameworks, and practices**, including a commitment to gender equality. Respective agencies should initiate a process that critically analyzes cyber-related policies from an intersectional perspective and include a cyber dimension into frameworks relevant to gender.[133]

Current policy analyses are gender-blind and need to include more **robust gender analysis**. State agencies should collect sex- and gender-disaggregated data that meet the standards for evidence-based policy design. Gender analysis necessitates collecting data on gender and cybercrime more broadly and disaggregating analysis by gender, age, ethnicity, class, socio-economic background, and other relevant intersecting identities to identify trends relating to the types of crimes, victims, perpetrators, and resulting harm.[134]

States should **develop methodologies** that help document gendered harm, quantify and qualify harms and impacts, and identify macro-level trends. Such methodologies should consider the range and frequency of vulnerabilities that are present within the population—or if the breach only affects a particular sub-group, the range and frequency of vulnerabilities that are present within that sub-group.

Anti-cybercrime policy and legislation can exacerbate or introduce new gendered harms. States should draw on resources that help policy makers and implementers incorporate feminist methodologies, principles, and gender analyses, promote gender equality, and prevent cyber policies from unintentionally reinforcing gender disparities.[135]

Participatory and inclusive approaches help states to fill potential gaps within the gender analysis, and to understand local and contextual gender dimensions. This includes engaging with gender and human rights groups, research institutions, and grassroots organizations with established networks and proximity to victims to encourage proportional representation of women and gendered perspectives throughout the policymaking and implementation process. Stakeholders should be formally involved to advise and provide evidence and insight.

Build Capacities and Avenues for Recourse and Justice

The **criminal justice system** needs substantial capacity to evidence and investigate the gendered impacts of data weaponization. Specialized training for law enforcement, prosecutors, and judges is critical to supporting the effective handling of cybercrime cases, ensuring that they have the technical capacity and expertise to secure and verify evidence, conduct thorough investigations, and prosecute offenders in a manner that upholds justice and protects victims of cybercrimes. States should increase the capacity of the institutions and agencies responsible for countering and responding to cybercrime and further embed gender considerations in their mandates, processes, and practices.

Victim assistance services should be systematically funded, and states should increase the capacity to provide gender-sensitive and responsive assistance that prioritizes a victim-centered approach to redress and reparations. States should create specialized cyber victim support units within law enforcement agencies that focus on supporting victims of cybercrime, with a particular emphasis on crimes that have a gendered component. Support for victims of gendered cyberattacks and other forms of technology-facilitated violence is currently fragmented, relying on a patchwork of civil society organizations and social justice groups. These organizations remain underfunded to provide comprehensive assistance, which is essential for addressing the complex needs of victims. This includes access to legal counsel, psychological support, and effective remedies that prevent revictimization.

States should create **online reporting mechanisms and helplines** that are accessible, safe, and specialized and allow the authorities to initiate investigation and recourse for victims. Such mechanisms should serve as a gateway to obtaining protection, accessing counseling, and finding support for removing harmful materials. States and private entities should prioritize initiatives and tools that address taking down sensitive data and harmful content. These are particularly relevant for medical and personal information and image-based abuse such as nonconsensual intimate images. Coalitions built across stakeholder groups, leveraging the strengths of states, the private sector, and civil society, should formalize knowledge and information sharing about cyber victimization.

Bolster Data Protection and Retention Rules

As long as organizations keep collecting troves of sensitive data, malicious actors are motivated to weaponize it against the targets. It is imperative that organizations limit the amount of sensitive data they collect. **Data collection and retention practices** must be in line with the principles of necessity, proportionality, and data minimization. Unless states have included these obligations directly into their national laws, the private sector has few binding obligations to follow human-rights-centered and gender-sensitive considerations.

All entities collecting personal data should adopt a **privacy-by-design approach**. Service providers should implement best practices on how to collect, use, and store data; only collect data that is essential to ensure the provision of the required service; and use it for purposes for which they obtained user consent. The sensitivity of data being processed must also be considered and restrictions increased based on potential risk. Risk analysis should incorporate social aspects and considerations based on gender and other intersectional identities.[136]

Norms and standards for data privacy should be considered in terms of the individuals and communities they affect. Public and private entities collecting, processing, storing, or otherwise handling or using personal data should prioritize working with users from targeted and marginalized communities, and consider their processes and practices through the lens of gender and intersectional identities. Designing from the margins can maximize safety, privacy, and security for all users, particularly those who are the most exposed.[137]

Secure Infrastructure and Design of Technology Products

Although technology design plays a key part in generating and enabling gendered harms in data weaponization, it also has a role in mitigating them. Technology should be designed, developed, and deployed with an **impact assessment** that considers context and identity.[138] Platforms and applications should include privacy-enhancing tools such as early warning systems through which incidents can be reported and identified.

Products should be built safely and securely, especially if integrated into critical infrastructure and services where data breaches have both national security and individual harm implications. As data breaches exploiting vendors of technology are increasing, data protection must be addressed already on the infrastructure and software layer on which the systems operate. Vulnerability analysis often leads to victim-blaming or attributing cyber incidents excessively to the "human error."[139] However, these are symptoms of systemic problems, rather than individual failures. The Security by Design approach to software security pioneered by the U.S. Cybersecurity and Infrastructure Security Agency provides key considerations for securing vulnerable software before it reaches people.[140]

Critical infrastructure should be designated in a way that includes services and facilities essential for people of all genders, gender identities and expressions, and sexual orientations. States should facilitate inclusive processes that allow for a critical assessment of remaining gray areas, such as the security and availability of essential facilities, assistance, and information related to gender-specific needs. Inclusive and participatory processes help to increase knowledge and coordination across different agencies and organizations and avoid contradictions in policy and practice.

Conclusion

> *Why and how are we using technology? What happens to us when we do? How is technology being used against us? And what is the recourse to justice?*

Cyber harm is not gender-blind, nor should be the responses that address it. This paper has argued that several types of data weaponization disproportionately affect women and gender and sexual minorities—highlighting that cybersecurity is not merely a technical issue, but also a deeply personal one. Different perceptions, norms, and roles, along with the systemic inequities reinforcing discrimination within the structures of states and societies, create and exacerbate gendered harm. The negative impacts are extensive and nonexhaustive. While experienced individually, gendered harms affect and stigmatize whole communities.

Since the nature and impacts of data weaponization are shaped by identity and environment, law, regulation, implementation, and design must reflect the lived realities of those affected. Feminist, gender-sensitive, and inclusive approaches can elevate the views and experiences of targeted and marginalized individuals to the forefront, offering a broader and, at the same time, deeper analysis that enables informed and effective interventions. Such frameworks present an alternative, intersectional analysis beyond traditional policy thinking and challenge dominant narratives about cybercrime and cybersecurity. Amplifying diverse voices is not merely a choice; it is essential for forging a safer, more just digital future.

Notes

[1] Samuel Wairimu and Lothar Fritsch, “Modelling Privacy Harms of Compromised Personal Medical Data: Beyond Data Breach,” *Proceedings of the 17th International Conference on Availability, Reliability and Security* 133 (2022): 1–9, https://doi.org/10.1145/3538969.3544462.

[2] Already three pieces of personal data—such as gender, date of birth, and zip code—can provide enough information to uniquely identify most individuals. These data are “quasi-identifiers”: attributes that do not uniquely identify individuals on their own. Nevertheless, once someone combines them with other quasi-identifiers or other data, they can narrow down the possible individuals to the point of uniquely identifying the individual. Constantinos Patsakis and Nikolaus Lykousas, “Man vs. the Machine in the Struggle for Effective Text Anonymisation in the Age of Large Language Models,” *Scientific Reports* 13, no. 16026 (2023), https://doi.org/10.1038/s41598-023-42977-3.

[3] Violeta Lyskoit, “Sensitive Data,” NordVPN, June 9, 2024, https://nordvpn.com/blog/sensitive-data/.

[4] Sourya Joyee De and Daniel Le Métayer, *PRIAM: A Privacy Risk Analysis Methodology* (Inria Research Centre Grenoble – Rhône-Alpes, 2016), https://inria.hal.science/hal-01302541/document.

[5] Wairimu and Fritsch, “Modelling Privacy Harms of Compromised Personal Medical Data,” https://doi.org/10.1145/3538969.3544462.

[6] Rebecca Emerson-Keeler, Amrit Swali, and Esther Naylor, *Integrating Gender in Cybercrime Capacity-Building: A Toolkit* (Chatham House, 2023), https://www.chathamhouse.org/sites/default/files/2023-07/2023-07-05-integrating-gender-in-cybercrime-capacity-building-emerson-keeler-et-al.pdf.

[7] Chatham House Cyber Policy team, *Gender Mainstreaming and the Proposed Cybercrime Convention: Commentary on the Consolidated Draft* (Chatham House, 2022), https://www.chathamhouse.org/sites/default/files/2022-12/2022-12-21-Gender-mainstreaming-and-the-proposed-cybercrime-convention.pdf.

[8] Emerson-Keeler, Swali, and Naylor, *Integrating Gender in Cybercrime Capacity-Building*, https://www.chathamhouse.org/sites/default/files/2023-07/2023-07-05-integrating-gender-in-cybercrime-capacity-building-emerson-keeler-et-al.pdf; Veronica Ferrari, Katharine Millar, Allison Pytlak, and Tatiana Tropina, *Inclusive Cyber Norms: A Toolkit* (Global Partners Digital, 2023), https://www.gp-digital.org/wp-content/uploads/2023/08/Inclusive-Cyber-Norms-Toolkit_GPD.pdf.

[9] Ferrari, Millar, Pytlak, and Tropina, *Inclusive Cyber Norms*, https://www.gp-digital.org/wp-content/uploads/2023/08/Inclusive-Cyber-Norms-Toolkit_GPD.pdf.

[10] James Shires, Bassant Hassib, and Amrit Swali, *Gendered Hate Speech, Data Breach, and State Overre ach* (Chatham House, 2024), https://www.chathamhouse.org/2024/05/gendered-hate-speech-data-breach-and-state-overreach.

[11] Divya Tiwari, “Data Breach Affects Women More, Has Chilling Effect on Their Online Participation,” BehanBox, December 6, 2023, https://behanbox.com/2023/12/06/data-breach-affects-women-more-has-chilling-effect-on-their-online-participation/.

[12] Chatham House Cyber Policy team, *Gender Mainstreaming and the Proposed Cybercrime Convention,* https://www.chathamhouse.org/sites/default/files/ 2022-12/2022-12-21-Gender-mainstreaming-and-the-proposed-cybercrime-convention.pdf.

[13] CyberPeace Institute, “Cyber Incident Tracer #Health,” CyberPeace Institute, https://cit.cyberpeaceinstitute.org.

[14] "Stolen Blood Test Data from Hospital Cyberattack Reportedly Published Online," ITV, June 22, 2024, https://www.itv.com/news/2024-06-21/nhs-cyber-attack-data-published-online-by-cyber-criminal-group; Denis Campbell and Dan Milmo, "Uk Government Weighs Action Against Russian Hackers over NHS Records Theft," *The Guardian*, June 21, 2024, https://www.theguardian.com/society/article/2024/jun/21/uk-national-crime-agency-russian-ransomware-hackers-qilin-nhs-patient-records.

[15] Bill Toulas, "BORN Ontario Child Registry Data Breach Affects 3.4 million People," Bleeping Computer, September 25, 2023, https://www.bleepingcomputer.com/news/security/born-ontario-child-registry-data-breach-affects-34-million-people/.

[16] Ax Sharma, "SickKids Impacted by Born Ontario Data Breach That Hit 3.4 Million," Bleeping Computer, September 26, 2023, https://www.bleepingcomputer.com/news/security/sickkids-impacted-by-born-ontario-data-breach-that-hit-34-million/.

[17] Katie Dangerfield, "BORN Ontario Data Breach Left Health Data of Millions Exposed. What Went Wrong?," Global News, September 26, 2023, https://globalnews.ca/news/9985743/born-ontario-health-data-breach/.

[18] Samuel Wairimu and Lothar Fritsch, "Modelling Privacy Harms of Compromised Personal Medical Data - Beyond Data Breach," https://dl.acm.org/doi/fullHtml/10.1145/3538969.3544462.

[19] "Almost 200 Patients at Major Melbourne Hospital Caught Up in Data Leak," 9News, October 5, 2023, https://www.9news.com.au/national/data-breach-royal-womens-hospital-melbourne-victoria-health-news/74175702-20e2-4ca7-818c-6695aa6edaa9.

[20] Allison Pytlak and Deborah Brown, *Why Gender Matters in International Cyber Security* (Women's International League for Peace and Freedom and the Association for Progressive Communications, April 2020), https://reachingcriticalwill.org/images/documents/Publications/gender-cybersecurity.pdf.

[21] Todd Shryock, "Patient Data Breaches Doubled in 2023," Medical Economics, October 23, 2023, https://www.medicaleconomics.com/view/patient-data-breaches-doubled-in-2023; Sophos X-Ops, "Turning the Screws: The Pressure Tactics of Ransomware Gangs," Sophos News, August 6, 2024, https://news.sophos.com/en-us/2024/08/06/turning-the-screws-the-pressure-tactics-of-ransomware-gangs/; Alejandro H. Cruz, Sara A. Arrow, and Sean Lau, "Recent Ransomware Attacks Highlight the Evolving Challenges in Responding to Cyber Extortion," *Data Security Law* (blog), Patterson Belknap, April 22, 2024, https://www.pbwt.com/data-security-law-blog/recent-ransomware-attacks-highlight-the-evolving-challenges-in-responding-to-cyber-extortion.

[22] Stuart E. Madnick, "The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase,"Apple News Room, December 2023, https://www.apple.com/newsroom/pdfs/The-Continued-Threat-to-Personal-Data-Key-Factors-Behind-the-2023-Increase.pdf.

[23] Alexander Martin, "Ransomware Gang Posts Breast Cancer Patients' Clinical Photographs," The Record, March 6, 2023, https://therecord.media/ransomware-lehigh-valley-alphv-black-cat.

[24] Owen Wong, *Cyberwarfare: The "Pink Tax" of Hacking* (Centre for International and Defence Policy, Queen's University, 2024), https://www.queensu.ca/cidp/publications/policy-briefs/cyberwarfare-pink-tax-hacking.

[25] Damien Pearse, "Anonymous Hacker Planned to Publish Details of Women Who Had Abortions," *The Guardian*, March 10, 2012, https://www.theguardian.com/uk/2012/mar/10/anonymous-hacker-women-abortion.

[26] James Griffiths, “HIV Status of over 14,000 People Leaked Online, Singapore Authorities Say,” CNN, January 28, 2019, https://edition.cnn.com/2019/01/28/health/hiv-status-data-leak-singapore-intl/index.html.

[27] “Mikhy Farrera-Brochez: U.S. Man Guilty of Trying to Extort Singapore over HIV Data,” BBC News, June 5, 2019, https://www.bbc.com/news/world-asia-48523308.

[28] Sharanjit Leyl, “Singapore HIV Data Leak Shakes a Vulnerable Community,” BBC News, February 22, 2019, https://www.bbc.com/news/world-asia-47288219; Beh Lih Yi, “LGBT+ People in Singapore ‘More Fearful’ after HIV Data Leak,” Reuters*,* January 29, 2019, https://jp.reuters.com/article/us-singapore-health-lgbt-idUSKCN1PN1NA/.

[29] Katharine Kemp, “Popular Fertility Apps Are Engaging in Widespread Misuse of Data, Including on Sex, Periods, and Pregnancy,” *University of New South Wales* Newsroom, March 22, 2023, https://www.unsw.edu.au/newsroom/news/2023/03/popular-fertility-apps-are-engaging-in-widespread-misuse-of-data; Kari Paul, “How Private Is Your Period-Tracking App? Not Very, Study Reveals,” *The Guardian*, August 17, 2022, https://www.theguardian.com/world/2022/aug/17/pregnancy-period-tracking-apps-privacy.

[30] “Period Trackers to Be Reviewed over Data Concerns,” BBC News, September 7, 2023, https://www.bbc.com/news/technology-66740184.

[31] Ashley Boyd, “Why Mozilla Is Scrutinizing the Privacy of Pregnancy Apps,” Mozilla Foundation, August 17, 2022, https://foundation.mozilla.org/en/blog/why-mozilla-is-scrutinizing-the-privacy-of-pregnancy-apps.

[32] Nina Bernarding and Vivienne Kobel, *Feminist Perspectives on the Militarisation of Cyberspace* (Centre for Feminist Foreign Policy, 2023), https://centreforfeministforeignpolicy.org/2023/06/21/feminist-perspectives-on-the-militarisation-of-cyberspace/.

[33] Shires, Hassib, and Swali, *Gendered Hate Speech, Data Breach, and State Overreach,* https://www.chathamhouse.org/2024/05/gendered-hate-speech-data-breach-and-state-overreach.

[34] Bernarding and Kobel, *Feminist Perspectives on the Militarisation of Cyberspace,* https://centreforfeministforeignpolicy.org/2023/06/21/feminist-perspectives-on-the-militarisation-of-cyberspace/.

[35] Flora Garamvolgyi, “Why U.S. Women Are Deleting Their Period Tracking Apps,” *The Guardian*, June 28, 2022, https://www.theguardian.com/world/2022/jun/28/why-us-woman-are-deleting-their-period-tracking-apps.

[36] Jennifer Gollan, “Websites Selling Abortion Pills Are Sharing Sensitive Data With Google,” *Ms. Magazine*, January 18, 2023, https://msmagazine.com/2023/01/18/google-abortion-pills-privacy-data/.

[37] “S.T.O.P. Releases Report On Abortion Surveillance After Roe*,*” Surveillance Technology Oversight Project, May 24, 2022, https://www.stopspying.org/latest-news/2022/5/24/stop-releases-report-on-abortion-surveillance-after-roe.

[38] Shires, Hassib, and Swali, *Gendered Hate Speech, Data Breach, and State Overreach,* https://www.chathamhouse.org/2024/05/gendered-hate-speech-data-breach-and-state-overreach.

[39] “Hackers Release Israeli LGBTQ Dating Site Details,” Radio France Internationale, November 2, 2021, https://www.rfi.fr/en/business-and-tech/20211102-hackers-release-israeli-lgbtq-dating-site-details; TOI Staff, “Hackers Claim to Leak Details of LGBTQ Dating Site After Ransom Not Paid,” *Times of Israel*, November 2, 2021, https://www.timesofisrael.com/hackers-claim-to-leak-details-of-lgbtq-dating-site-after-ransom-not-paid/.

40 Jen Caltrider, Misha Rykov, and Zoë MacDonald, "Data-Hungry Dating Apps Are Worse Than Ever for Your Privacy," Mozilla Foundation, April 23, 2024, https://foundation.mozilla.org/en/privacynotincluded/articles/data-hungry-dating-apps-are-worse-than-ever-for-your-privacy/.

41 Insikt Group, *Cyber Threat Analysis: Online Surveillance, Censorship, and Discrimination for LGBTQIA+ Community Worldwide* (Recorded Future, 2020), https://go.recordedfuture.com/hubfs/reports/cta-2020-0714.pdf.

42 Article 19, *LGBTQ Online Summary Report: Apps, Arrests, and Abuse in Egypt, Lebanon, and Iran* (Article 19, February 2018), https://www.article19.org/wp-content/uploads/2018/02/LGBTQ-Apps-Arrest-and-Abuse-report_22.2.18.pdf; Human Rights Watch (HRW), *All This Terror Because of a Photo: Digital Targeting and Its Offline Consequences for LGBT People in the Middle East and North Africa* (HRW, February 21, 2023), https://www.hrw.org/report/2023/02/21/all-terror-because-photo/digital-targeting-and-its-offline-consequences-lgbt.

43 Natasha Culzac, "Egypt's Police Using Social Media and Apps Like Grindr to Trap Gay People," *The Independent*, September 17, 2014, https://www.independent.co.uk/news/world/africa/egypt-s-police-using-social-media-and-apps-like-grindr-to-trap-gay-people-9738515.html.

44 Article 19, *LGBTQ Online Summary Report*, https://www.article19.org/wp-content/uploads/2018/02/LGBTQ-Apps-Arrest-and-Abuse-report_22.2.18.pdf; Human Rights Watch, *All This Terror Because of a Photo*, https://www.hrw.org/report/2023/02/21/all-terror-because-photo/digital-targeting-and-its-offline-consequences-lgbt.

45 Byron Tau, "Grindr User Data Was Sold Through Ad Networks," *Wall Street Journal,* May 2, 2022, https://www.wsj.com/articles/grindr-user-data-has-been-for-sale-for-years-11651492800.

46 Andy Greenberg, "Gay Dating Apps Promise Privacy, But Leak Your Exact Location," *Wired*, May 20, 2016, https://www.wired.com/2016/05/grindr-promises-privacy-still-leaks-exact-location/; Article 19, "Apps and Traps: Dating Apps Must Do More to Protect LGBTQ Communities in Middle East and North Africa," Article 19, January 22, 2018, https://www.article19.org/resources/apps-traps-dating-apps-must-protect-communities-middle-east-north-africa/.

47 "13 Manifestations of GBV Using Technology," *Take Back the Tech* (blog), August 17, 2018, https://www.takebackthetech.net/blog/13-manifestations-gbv-using-technology; Tanisha Ranjit and Shraddha Mahilkar, *Online Gender-Based Violence: And Its Impact On The Civic Freedoms of Women Human Rights Defenders in the Indo-Pacific*, (International Center for Not-for-Profit Law, March 2023), https://www.icnl.org/wp-content/uploads/Online-Gender-Based-Violence-report-final.pdf; Shires, Hassib, and Swali, *Gendered Hate Speech, Data Breach, and State Overreach,* https://www.chathamhouse.org/2024/05/gendered-hate-speech-data-breach-and-state-overreach.

48 "'Stalker' Rap After Hospital Data Breach," *Cumnock Chronicle*, December 2018, https://www.cumnockchronicle.com/news/17310994.stalker-rap-hospital-data-breach.

49 Information and Privacy Commission, New South Wales, *Guidelines on the Assessment of Data Breaches Under Part 6A of the PPIP Act.*

50 "ICO Case Reference Number: INV/0113/2022," Information Commissioner's Office, September 22, 2022, https://ico.org.uk/media/action-weve-taken/reprimands/4023136/wakefield-council-reprimand.pdf; Robert Booth, "Data Breaches Putting Domestic Abuse Victims' Lives At Risk, Says U.K. Watchdog," *The Guardian*, September 27, 2023, https://www.theguardian.com/society/2023/sep/27/data-breaches-putting-domestic-abuse-victims-lives-at-risk-says-uk-watchdog; Christine Sabino, "Victims of Domestic Abuse Put at Risk of Harm by Data

Breaches," Hayes Connor Solicitors, September 28, 2023, https://www.hayesconnor.co.uk/news-resources/news/victims-of-domestic-abuse-put-at-risk-of-harm-by-data-breaches/.

51 Allison Pytlak and Deborah Brown, "Why Gender Matters in International Cyber Security," Reaching Critical Will, April 2020, https://www.reachingcriticalwill.org/resources/publications-and-research/publications/14677-why-gender-matters-in-international-cyber-security.

52 Research and Trend Analysis Branch, *Killings of Women and Girls by Their Intimate Partner or Other Family Members: Global Estimates 2020* (United Nations Office on Drugs and Crime, November 2021), https://www.unodc.org/documents/data-and-analysis/statistics/crime/UN_BriefFem_251121.pdf.

53 "Interview: How Turkey's Failure to Protect Women Can Cost Them Their Lives," Human Rights Watch, March 26, 2022, https://www.hrw.org/news/2022/05/26/interview-how-turkeys-failure-protect-women-can-cost-them-their-lives; Pytlak and Brown, "Why Gender Matters in International Cyber Security," https://www.reachingcriticalwill.org/resources/publications-and-research/publications/14677-why-gender-matters-in-international-cyber-security; Zeynep Tufekci, "WikiLeaks Put Women in Turkey in Danger, for No Reason (UPDATE)," *Huffington Post*, December 6, 2017, https://www.huffpost.com/entry/wikileaks-erdogan-emails_b_11158792; Jesse Singal, "Why Did WikiLeaks Help Dox Most of Turkey's Adult Female Population?," *New York Magazine*, July 27, 2016, https://nymag.com/intelligencer/2016/07/why-did-wikileaks-help-dox-most-of-turkeys-adult-female-population.html.

54 Aurelija Skebaite, "The 20 Biggest Data Breaches in History," NordVPN, August 21, 2024, https://nordvpn.com/blog/biggest-data-breaches/.

55 Patrick Smith and Jason Abbruzzese, "AT&T Says Hackers Stole Records of Nearly All Cellular Customers' Calls and Texts," NBC News, July 12, 2024, https://www.nbcnews.com/news/us-news/t-says-hackers-stole-records-nearly-cell-customers-calls-texts-rcna161507.

56 Chatham House Cyber Policy team, *Gender Mainstreaming and the Proposed Cybercrime Convention,* https://www.chathamhouse.org/sites/default/files/ 2022-12/2022-12-21-Gender-mainstreaming-and-the-proposed-cybercrime-convention.pdf.

57 Asher Flynn, Anastasia Powell, and Sophie Hindes, "An Intersectional Analysis of Technology-Facilitated Abuse: Prevalence, Experiences and Impacts of Victimization," *British Journal of Criminology*, 64, no. 3 (May 2024): 600–619, https://doi.org/10.1093/bjc/azad044; Sara Seppanen, "LGBTQ+ Community Grapples with Hidden Wave of Digital Abuse," Binding Hook, March 6, 2024, https://bindinghook.com/articles-binding-edge/lgbtq-community-grapples-with-hidden-wave-of-digital-abuse/.

58 Christopher Parsons, Adam Molnar, Jakub Dalek et al., *The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry* (Citizen Lab, June 12, 2019), https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisciplinary-assessment-of-the-stalkerware-application-industry/.

59 Sofia Celi, Juliana Guerra, and Mallory Knodel, *Intimate Partner Violence Digital Considerations* (Internet Engineering Task Force, October 18, 2023), https://www.ietf.org/archive/id/draft-irtf-hrpc-ipvc-00.html.

60 Alex Scroxton, "Use of Abusive Stalkerware Against Women Skyrocketed in 2020," *Computer Weekly*, November 25, 2020, https://www.computerweekly.com/news/252492575/Use-of-abusive-stalkerware-against-women-skyrocketed-in-2020.

61 Laura O'Brien, Felicia Anthonio, Peter Micek, Rand Hammoud, and Marwa Fatafta, "Silenced, Spied On, and Stalked: Why We're Taking the Fight

for Gender Equality to the UN," Access Now, March 19, 2023, https://www.accessnow.org/silenced-spied-on-and-stalked-why-were-taking-the-fight-for-gender-equality-to-the-un/.

62 Celi, Guerra, and Knodel, *Intimate Partner Violence Digital Considerations,* https://www.ietf.org/archive/id/draft-irtf-hrpc-ipvc-00.html.

63 Andi Brown, Diarmaid Harkin, and Leonie Maria Tanczer, "Safeguarding the 'Internet of Things' for Victim-Survivors of Domestic and Family Violence: Anticipating Exploitative Use and Encouraging Safety-by-Design," *Violence Against Women* 2024), https://doi.org/10.1177/10778012231222486.

64 Julia Slupska and Leonie Maria Tanczer, *International Handbook of Technology-Facilitated Violence and Abuse* (Emerald, June 4, 2021).

65 Delanie Woodlock, "The Abuse of Technology in Domestic Violence and Stalking," *Violence Against Women* 23, no. 5 (2017): 584–602, https://doi.org/10.1177/1077801216646277; Celi, Guerra, and Knodel, *Intimate Partner Violence Digital Considerations,* https://www.ietf.org/archive/id/draft-irtf-hrpc-ipvc-00.html.

66 Alfred Ng, "Texas Sues General Motors Over Car Data Tracking," *Politico*, August 13, 2024, https://www.politico.com/news/2024/08/13/texas-general-motors-car-data-tracking-00173877.

67 Shires, Hassib, and Swali, *Gendered Hate Speech, Data Breach, and State Overreach,* https://www.chathamhouse.org/2024/05/gendered-hate-speech-data-breach-and-state-overreach.

68 Kristine Baekgaard, *Technology-Facilitated Gender-Based Violence An Emerging Issue in Women, Peace, and Security* (Georgetown Institute for Women, Peace, and Security, 2024), https://giwps.georgetown.edu/wp-content/uploads/2024/06/Technology-Facilitated-Gender-Based-Violence.pdf.

69 Bernarding and Kobel, *Feminist Perspectives on the Militarisation of Cyberspace*, https://centreforfeministforeignpolicy.org/2023/06/21/feminist-perspectives-on-the-militarisation-of-cyberspace/.

70 Hagar Shezaf and Jonathan Jacobson "Israel's Cyber Spy Industry Helps World Dictators Hunt Dissidents and Gays," *Haaretz*, October 20, 2018, https://www.haaretz.com/israel-news/2018-10-20/ty-article-magazine/.premium/israels-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays/0000017f-e9a9-dc91-a17f-fdadde240000.

71 Marcus Michaelsen, "Is Digital Transnational Repression "Spreading" Among States?" *Global Policy Journal* (blog), March 21, 2023, https://www.globalpolicyjournal.com/blog/21/03/2023/digital-transnational-repression-spreading-among-states.

72 Tiwari, "Data Breach Affects Women More, " https://behanbox.com/2023/12/06/data-breach-affects-women-more-has-chilling-effect-on-their-online-participation/.

73 John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert, "Reckless Exploit Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware," Citizen Lab, June 19, 2017, https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/.

74 Human Rights Council, Reinforcing Media Freedom and the Safety of Journalists in the Digital Age: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression(UN General Assembly, April 20, 2022), https://www.undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F50%2F29.

75 "Safety of Women and Nonbinary Journalists On and Offline," Committee to Protect Journalists, https://cpj.org/campaigns/safety-women-nonbinary-journalists-online-offline/.

[76] Julie Posetti, Nabeelah Shabbir, Diana Maynard, Kalina Bontcheva, and Nermine Aboulez, *The Chilling: Global Trends in Online Violence Against Women Journalists* (UNESCO, 2021), https://unesdoc.unesco.org/ark:/48223/pf0000377223.

[77] Marwa Fatafta, "Unsafe Anywhere: Women Human Rights Defenders Speak Out About Pegasus Attacks," Access Now, January 17, 2022, https://www.accessnow.org/women-human-rights-defenders-pegasus-attacks-bahrain-jordan/.

[78] Phineas Rueckert, "Pegasus: The New Global Weapon for Silencing Journalists," Forbidden Stories, July 18, 2021, https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/.

[79] O'Brien, Anthonio, Micek, Hammoud, and Fatafta, "Silenced, Spied On, and Stalked," https://www.accessnow.org/silenced-spied-on-and-stalked-why-were-taking-the-fight-for-gender-equality-to-the-un/.

[80] Stephanie Kirchgaessner and Andrew Roth, "Exiled Russian Journalist Hacked Using NSO Group Spyware," *The Guardian*, September 13, 2023, https://www.theguardian.com/technology/2023/sep/13/exiled-russian-journalist-galina-timchenko-reportedly-hacked-using-nso-group-spyware; Julie Posetti and Nabeelah Shabbir, *The Chilling: A Global Study of Online Violence Against Women Journalists* (International Center for Journalists, November 2, 2022), https://www.icfj.org/sites/default/files/2022-11/ICFJ_UNESCO_The%20Chilling_2022_1.pdf.

[81] "Personal Information of Hundreds of Mexican Journalists Exposed in Government Data Leak," Committee to Protect Journalists, February 1, 2021, https://cpj.org/2024/02/personal-information-of-hundreds-of-mexican-journalists-exposed-in-government-data-leak/.

[82] Siria Gastelum Felix, "Journalism Still Deadly in Mexico," Global Initiative Against Transnational Organized Crime, March 28, 2024, https://globalinitiative.net/analysis/journalism-still-deadly-in-mexico/.

[83] Lucía Lagunes Huerta et al., *Palabras Impunes: Estigmatización Y Violencia: Contra Mujeres Periodistas en México 2019–2022* (Comunicación e Información de la Mujer A.C., 2022), https://cimac.org.mx/wp-content/uploads/2022/11/Informe_CIMAC_2022_AMLO_Estigmatizacion.pdf.

[84] Azadeh Akbari, *Authoritarian Smart City: A Research Agenda* (University of Twente, December 16, 2022), https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/15964.

[85] Bernarding and Kobel, *Feminist Perspectives on the Militarisation of Cyberspace,* https://centreforfeministforeignpolicy.org/2023/06/21/feminist-perspectives-on-the-militarisation-of-cyberspace/.

[86] For example, Falastine Saleh and Esra'a Al Shafei's paper also shows how the localized use of Israeli surveillance technologies in Palestine contribute to widespread acceptance and global adoption of such oppressive practices. See Esra'a Al Shafei and Falastine Saleh, "Surveillance as a Service: The Global Impact of Israeli 'Defense' Technologies on Privacy and Human Rights," *Tor Project* (blog), April 8, 2024, https://blog.torproject.org/surveillance-as-a-service-global-impact-of-israeli-defense-technologies-on-privacy-human-rights/.

[87] Sarah Shoker, *Making Gender Visible in Digital ICTs and International Security* (Global Affairs Canada, April 2020), https://front.un-arm.org/wp-content/uploads/2020/04/commissioned-research-on-gender-and-cyber-report-by-sarah-shoker.pdf; Sarah Sobieraj, "Bitch, Slut, Skank, Cunt: Patterned Resistance to Women's Visibility in Digital Publics," *Information, Communication & Society*, 21 (11): 2017, 1–15, https://doi.org/10.1080/1369118X.2017.1348535.

[88] Olivia Solon, "'I Will Not Be Silenced': Women Targeted in Hack-and-Leak Attacks Speak Out About Spyware," NBC News, August 1, 2021, https://

www.nbcnews.com/tech/social-media/i-will-not-be-silenced-women-targeted-hack-leak-attacks-n1275540.

[89] "Who We Are," #ShePersisted, https://she-persisted.org/who-we-are/.

[90] Shoker, *Making Gender Visible*, https://front.un-arm.org/wp-content/uploads/2020/04/commissioned-research-on-gender-and-cyber-report-by-sarah-shoker.pdf.

[91] Lucina Di Meco and Kristina Wilfore, "Gendered Disinformation Is a National Security Problem," Brookings, March 8, 2021, https://www.brookings.edu/articles/gendered-disinformation-is-a-national-security-problem/.

[92] Special Committee on Foreign Interference in all Democratic Processes in the European Union, *Report on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation* (European Union, February 8, 2022), https://www.europarl.europa.eu/doceo/document/A-9-2022-0022_EN.html.

[93] "How Women Are Singled Out for Vile Abuse for Political Ends," *The Economist*, November 7, 2019, https://www.economist.com/europe/2019/11/07/how-women-are-singled-out-for-vile-abuse-for-political-ends.

[94] Jessikka Aro, "How Pro-Russian Trolls Tried to Destroy Me," BBC News, October 6, 2017, https://www.bbc.com/news/blogs-trending-41499789.

[95] Pavlina Pavlova, "Gendered Disinformation and Connected Cyber Threats: Historical Patterns, New Battlefields, and the Implications for International Security," *Global Policy Journal* (blog), February 27, 2023, https://www.globalpolicyjournal.com/blog/27/02/2023/gendered-disinformation-and-connected-cyber-threats-historical-patterns-new; Jim Waterson, "British Female Politicians Targeted by Fake Pornography," *The Guardian*, July 1, 2024, https://www.theguardian.com/technology/article/2024/jul/01/british-female-politicians-targeted-by-fake-pornography.

[96] Mark Scott, "Deepfake Porn is Political Violence," *Politico*, February 8, 2024, https://www.politico.eu/newsletter/digital-bridge/deepfake-porn-is-political-violence/.

[97] Seb Starcevic, "Italy's Giorgia Meloni Called to Testify in Deepfake Porn Case," *Politico*, March 21, 2024, https://www.politico.eu/article/italian-pm-giorgia-meloni-called-to-testify-in-deepfake-porn-case/.

[98] Nina Jankowicz, Jillian Hunchak, Alexandra Pavliuc, et al., *Malign Creativity: How Gender, Sex, and Lies are Weaponized Against Women Online* (Wilson Center, January 2021), https://www.wilsoncenter.org/publication/malign-creativity-how-gender-sex-and-lies-are-weaponized-against-women-online.

[99] Karen Tumulty, Kate Woodsome, and Sergio Peçanha, "How Sexist, Racist Attacks on Kamala Harris Have Spread Online – A Case Study," *Washington Post*, October 7, 2020, https://www.washingtonpost.com/opinions/2020/10/07/kamala-harris-sexist-racist-attacks-spread-online/; Prithvi Iyer, "The Surge of Gendered and Racial Attacks on Kamala Harris was Predictable. Social Media Platforms Still Aren't Prepared," Tech Policy Press, July 24, 2024, https://www.techpolicy.press/the-surge-of-gendered-and-racial-attacks-on-kamala-harris-was-predictable-social-media-platforms-still-arent-prepared/; "Deepfake Claiming Kamala Harris Was a Sex Worker Circulating Less than a Day After Her First Rally," Euronews, July 24, 2024, https://www.euronews.com/next/2024/07/24/deepfake-claiming-kamala-harris-was-a-sex-worker-circulating-less-than-a-day-after-her-fir.

[100] A.W. Ohlheiser, "How Much More Abuse Do Female Politicians Face? A Lot," *MIT Technology Review*, October 6, 2020, https://www.technologyreview.com/2020/10/06/1009406/twitter-facebook-online-harassment-politicians/;

Sandra Håkansson, “The Gendered Representational Costs of Violence Against Politicians,” *Perspectives on Politics* 22, no. 1 (2022): 81–96, https://doi.org/10.1017/S1537592723001913; “Gendered Disinformation in the European Parliamentary Elections,” *Global Disinformation Index* (blog), June 10, 2024, https://www.disinformationindex.org/blog/2024-06-10-gendered-disinformation-in-the-european-parliamentary-elections/.

101 Allison Pytlak and Lisa Sharland, “Narrowing the Gender Gap in Cyber Security,” Stimson Center, March 8, 2024, https://www.stimson.org/2024/narrowing-the-gender-gap-in-cyber-security/; Shires, Hassib, and Swali, *Gendered Hate Speech, Data Breach, and State Overreach,* https://www.chathamhouse.org/2024/05/gendered-hate-speech-data-breach-and-state-overreach.

102 “13 Manifestations of GBV Using Technology,” https://www.takebackthetech.net/blog/13-manifestations-gbv-using-technology.

103 Shires, Hassib, and Swali, *Gendered Hate Speech, Data Breach, and State Overreach,* https://www.chathamhouse.org/2024/05/gendered-hate-speech-data-breach-and-state-overreach.

104 “Egypt Woman Commits Suicide After Husband Threatens to Share Nude Pictures Online,” Middle East Monitor, February 2, 2022, https://www.middleeastmonitor.com/20220202-egypt-woman-commits-suicide-after-husband-threatens-to-share-nude-pictures-online/.

105 “Egypt: Online Extortion Is Another Motive for Suicide,” Alaraby, January 7, 2022, https://www.alaraby.co.uk/society/مصر-الابتزاز-الإلكتروني_دافع-آخر-للانتحار; “Basant Khaled: An Egyptian Girl Committed Suicide Due to ‘Blackmail and Fabricated Photos,’” BBC News, January 4, 2022, https://www.bbc.com/arabic/trending-59859876.

106 “Two Arrested in Egypt After Teenage Girl’s Suicide Sparks Outrage,” BBC News, January 4, 2022, https://www.bbc.com/news/world-middle-east-59868721; Habiba Abdelaal, *Cyber Violence and Women in Egypt* (Tahrir Institute for Middle East Policy, March 31, 2022), https://timep.org/2022/03/31/cyber-violence-and-women-in-egypt/.

107 Global Freedom of Expression, “The Case of the Egyptian TikTok Influencers,” Columbia University, https://globalfreedomofexpression.columbia.edu/cases/the-tiktok-girls-case/.

108 “2023 State of Deepfakes Realities: Threats, and Impact,” Security Hero, https://www.securityhero.io/state-of-deepfakes/.

109 Vandinika Shukla, “Deepfakes and Elections: The Risk to Women’s Political Participation,” Tech Policy Press, February 29, 2024, https://www.techpolicy.press/deepfakes-and-elections-the-risk-to-womens-political-participation/.

110 Lilian Coral, “Utilizing the Online Crowd: How Swifties Could Keep Us Safe From AI,” *The Thread* (blog), New America, February 2, 2024, https://www.newamerica.org/the-thread/taylor-swift-ai-deepfake-social-media/.

111 Nichola Kristof, “The Online Degradation of Women and Girls That We Meet with a Shrug,” *New York Times*, March 23, 2024, https://www.nytimes.com/2024/03/23/opinion/deepfake-sex-videos.html.

112 Aziz Z. Huq and Rebecca Wexler, “Digital Privacy for Reproductive Choice in the Post-Roe Era,” *New York University Law Review* 98, no. 2 (May 2023), https://nyulawreview.org/issues/volume-98-number-2/digital-privacy-for-reproductive-choice-in-the-post-roe-era/.

113 Sharona Coutts, “Anti-Choice Groups Use Smartphone Surveillance to Target ‘Abortion-Minded Women’ During Clinic Visits,” Rewire News Group, May 25, 2016, https://rewirenewsgroup.com/article/2016/05/25/anti-choice-groups-deploy-smartphone-surveillance-target-abortion-minded-women-clinic-visits/; Liam Stack, “A Brief History of Deadly Attacks

on Abortion Providers," *New York Times*, November 29, 2015, https://www.nytimes.com/interactive/2015/11/29/us/30abortion-clinic-violence.html; Sam Sabin, "'Lock It Down Right Now': Abortion Rights Advocates Prepare for a New Wave of Digital Security Threats," *Politico*, June 17, 2022, https://www.politico.com/news/2022/06/17/abortion-rights-advocates-digital-security-threats-00040654; Rebecca Grant, "The Disturbing Rise of Cyberattacks Against Abortion Clinics," *Wired*, October 5, 2017, https://www.wired.com/story/cyberattacks-against-abortion-clinics/.

114 Katie Klabusich, "Planned Parenthood Under Attack by Anti-Abortion Hackers, Politicians," *Rolling Stone,* July 31, 2015, https://www.rollingstone.com/politics/politics-news/planned-parenthood-under-attack-by-anti-abortion-hackers-politicians-71311/.

115 Shoker, *Making Gender Visible*, https://front.un-arm.org/wp-content/uploads/2020/04/commissioned-research-on-gender-and-cyber-report-by-sarah-shoker.pdf.

116 Rebecca Torrence, "Hack Targets Planned Parenthood, Exposing Personal Information of 400K Patients," Fierce Healthcare, December 3, 2021, https://www.fiercehealthcare.com/tech/hack-targets-planned-parenthood-data-from-400-000-patients.

117 Andy Greenberg, "Security News This Week: Data Brokers Track Abortion Clinic Visits for Anyone to Buy," *Wired*, May 7, 2022, https://www.wired.com/story/data-brokers-tracking-abortion-clinics-security-news/.

118 Joseph Cox, "Data Broker Is Selling Location Data of People Who Visit Abortion Clinics," *Vice*, May 3, 2022, https://www.vice.com/en/article/location-data-abortion-clinics-safegraph-planned-parenthood/; Joseph Cox, "Location Data Firm Provides Heat Maps of Where Abortion Clinic Visitors Live," *Vice*, May 5, 2022, https://www.vice.com/en/article/location-data-firm-heat-maps-planned-parenthood-abortion-clinics-placer-ai/.

119 James Factora, "TERFs Are Using Google Maps to Track and Target Trans Healthcare Providers," *Them*, September 28, 2022, https://www.them.us/story/terfs-google-maps-hospitals-community-centers.

120 Wong, *Cyberwarfare: The "Pink Tax" of Hacking,* https://www.queensu.ca/cidp/publications/policy-briefs/cyberwarfare-pink-tax-hacking.

121 "Human Rights Crisis: Abortion in the United States After Dobbs," Human Rights Watch, April 18, 2023, https://www.hrw.org/news/2023/04/18/human-rights-crisis-abortion-united-states-after-dobbs.

122 "Ciberataque A Sanitas: Impactos Diferenciales Sobre Mujeres Cuidadoras," Karisma Fundacion, March 3, 2024, https://web.karisma.org.co/ciberataque-a-sanitas-impactos-diferenciales-sobre-mujeres-cuidadoras/.

123 "UN Women Reveals Concerning Regression in Attitudes Towards Gender Roles During Pandemic in New Study," UN Women, June 22, 2022, https://www.unwomen.org/en/news-stories/press-release/2022/06/un-women-reveals-concerning-regression-in-attitudes-towards-gender-roles-during-pandemic-in-new-study; Clare Wenhman, *The Gendered Impact of the COVID-19 Crisis and Post-Crisis Period* (European Parliament Department for Citizens' Rights and Constitutional Affairs, September 2020), https://www.europarl.europa.eu/RegData/etudes/STUD/2020/658227/IPOL_STU(2020)658227_EN.pdf.

124 Wong, *Cyberwarfare: The "Pink Tax" of Hacking,* https://www.queensu.ca/cidp/publications/policy-briefs/cyberwarfare-pink-tax-hacking.

125 Jonathan Reed, "More School Closings Coast-to-Coast Due to Ransomware*," Security Intelligence*, March 27, 2023, https://securityintelligence.com/news/schools-closing-due-to-ransomware/.

126 Reed, “More School Closings Coast-to-Coast Due to Ransomware,” https://securityintelligence.com/news/schools-closing-due-to-ransomware/.

127 Wong, *Cyberwarfare: The “Pink Tax” of Hacking,* https://www.queensu.ca/cidp/publications/policy-briefs/cyberwarfare-pink-tax-hacking.

128 Bernarding and Kobel, *Feminist Perspectives on the Militarisation of Cyberspace*, https://centreforfeministforeignpolicy.org/2023/06/21/feminist-perspectives-on-the-militarisation-of-cyberspace/; Pytlak and Brown, *Why Gender Matters in International Cyber Security*, https://reachingcriticalwill.org/images/documents/Publications/gender-cybersecurity.pdf.

129 Wong, *Cyberwarfare: The “Pink Tax” of Hacking,* https://www.queensu.ca/cidp/publications/policy-briefs/cyberwarfare-pink-tax-hacking.

130 Shires, Hassib, and Swali, *Gendered Hate Speech, Data Breach, and State Overreach,* https://www.chathamhouse.org/2024/05/gendered-hate-speech-data-breach-and-state-overreach.

131 For example, in 2022, the same Russian hacking group that triggered the U.S. National Emergency when they shut down the Colonial pipeline leaked a dataset of Medibank customers entitled “Abortions.csv” after failing to receive a ransom payment. See Wong, *Cyberwarfare: The “Pink Tax” of Hacking,* https://www.queensu.ca/cidp/publications/policy-briefs/cyberwarfare-pink-tax-hacking.

132 Shoker, *Making Gender Visible*, https://front.un-arm.org/wp-content/uploads/2020/04/commissioned-research-on-gender-and-cyber-report-by-sarah-shoker.pdf.

133 For illustration, the EU directive against gender-based violence includes considerations for cyber violence. The Istanbul Convention on all forms of violence against women and domestic violence bears relevance for addressing online and technology-facilitated violence against women. The Budapest Convention on Cybercrime includes provisions for the nonconsensual sharing of intimate images, and its transposition into national law can elevate the importance of investigating and prosecuting these types of crime under the national criminal justice system.

134 For example, the *U.S. National Cyber Strategy* acknowledges that “the greatest harm falls upon the vulnerable populations for whom risks to personal data can produce disproportionate harm” and could include clearer identification of vulnerable groups and people in positions of vulnerability to adequately protect them. See Biden–Harris Administration, *National Cybersecurity Strategy* (White House, 2023), 19, https://www.whitehouse.gov/wp-content/uploads/ 2023/03/National-Cybersecurity-Strategy-2023.pdf.

135 Such guidance is provided, for example, in the Association for Progressive Communications’ tool for assessing the gender impact of national cybersecurity strategies and Chatham House’s strategic approach to countering cybercrime and their framework for integrating gender in cybercrime capacity-building. See Verónica Ferrari and Paula Martins, *A Framework for Developing Gender-Responsive Cybersecurity Policy: Assessment Tool* (Association for Progressive Communications, 2023), https://www.apc.org/sites/default/files/apcgendercyber-assessmenttool.pdf; Joyce Hakmeh and Jamie Saunders, *The Strategic Approach to Countering Cybercrime (SACC) Framework* (Chatham House, July 11, 2024), https://www.chathamhouse.org/2024/07/strategic-approach-countering-cybercrime-sacc-framework/introduction; Emerson-Keeler, Swali, and Naylor, *Integrating Gender in Cybercrime Capacity-Building*, https://www.chathamhouse.org/sites/default/files/2023-07/2023-07-05-integrating-gender-in-cybercrime-capacity-building-emerson-keeler-et-al.pdf.

136 For example, medical data is legally considered as a special category of personal data (i.e., sensitive)

under GDPR (Art. 9) and other privacy laws, for instance, the HIPAA Privacy Rule. The principle of data minimization is a key element of GDPR (Art. 5).

[137] Afsaneh Rigot, *Design from the Margins* (Harvard Kennedy School Belfer Center for Science and International Affairs, May 13, 2022), https://www.belfercenter.org/publication/design-margins.

[138] For example, developers of apps that collect sensitive data should not set localization functions as a default option and should consider disabling such functions if not necessary for the provided service. Health care app providers should refrain from collecting location-based information that tracks visits to abortion clinics and other gendered health care facilities.

[139] For example, phishing links are a common vector for malicious software.

[140] Cybersecurity and Infrastructure Security Agency (CISA), *Shifting the Balance of Cybersecurity Risk: Principles and Approached for Secure by Design Software* (CISA, 2023), https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf.