Gender perspectives on privacy: Submission to the United Nations Special Rapporteur on the right to privacy

Association for Progressive Communications (APC)

October 2018

Table of contents

1. Introduction

The Association for Progressive Communications (APC) is an international network and non-profit organisation founded in 1990 that works to help ensure everyone has affordable access to a free and open internet to improve lives, realise human rights and create a more just world. As an organisation that has worked at the intersections of women's rights, sexual rights and technology for more than two decades, we welcome the focus of the Special Rapporteur on the right to privacy on "gender perspectives on privacy".

The privacy violations that women and LGBTIQ persons[1] experience take place within a context of existing structural inequalities and discrimination which put them at particular risk of violence and other types of human rights violations. It is important to recognise, therefore, that for these communities, conversations about privacy cannot take place without also reflecting on the surveillance they face – by states and non-state actors, including in their intimate relationships, families, friendships, among others – on their immediate social environment. For APC, it is essential that considerations of privacy also take account of autonomy, bodily integrity, sexuality and sexual expression and include perspectives that relate to decision making over one's own personal data and information.

Privacy creates the necessary space for people who face discrimination or marginalisation based on their gender, sexual orientation, gender identity or expression, to fully enjoy their human rights.[2] This concept of privacy is not limited to private spaces but also extends to public spheres; for instance, people whose gender expression, identity and/or sexuality is apparent and visible or can be ascertained are entitled to the right to privacy in public spaces too.

APC encourages the Special Rapporteur to take an intersectional approach when considering gendered dimensions of privacy. Intersectionality as a framework gives visibility to and questions powers and privileges that emerge as a result of gender, race, ethnicity, class, and other social and cultural hierarchies.[3] Individuals and groups who are viewed as being situated lower in social and cultural hierarchies, or seen by society or the state as needing to be controlled, are afforded less privacy.

[1]In this submission we focus on the gendered dimensions of privacy as they affect people who identify as women, lesbian, gay, bisexual, queer, transgender and intersex. We do not explore privacy issues as they relate to girls.
[2]Nevertheless, a feminist perspective of the right to privacy highlights that historically, privacy has been used as a space where women face violence from their family, partners and others; this *darker zone of privacy* is a potential sphere to dominate, humiliate and degrade women.
[3]Vale, H. (2017). In plain sight: On sexuality, rights and the internet in India, Nepal and Sri Lanka. In Association for Progressive Communications, *EROTICS South Asia exploratory research: Sex, rights and the internet*. https://www.apc.org/sites/default/files/Erotics_1_FIND.pdf#page=6

Finally, we reiterate that privacy is a fundamental and universal right that should be enjoyed without discrimination by people of all genders. We encourage the Special Rapporteur to reject arguments that invoke privacy such as the privacy of the home or the protection of the family that could be used to shield human rights violations occurring in private settings.

2. Gender and privacy in international human rights standards

The right to privacy is a fundamental right enshrined by the Universal Declaration of Human Rights (hereinafter, "UDHR"), the International Covenant on Civil and Political Rights, and a number of regional human rights instruments. Everyone is entitled to all the rights and freedoms set forth in the UDHR, without distinction of any kind.

In recent years, the UN has given considerable attention to the right to privacy in the digital age, in particular to issues around mass surveillance by governments and companies. This is not surprising, since the revelations of Edward Snowden were the impetus for the first UN General Assembly (hereinafter, "UNGA") resolution on the right to privacy in the digital age in 2014.[4] Since then the Office of the High Commissioner for Human Rights has issued two reports[5][6] addressing challenges to the right to privacy in light of technological advances, and UNGA and the Human Rights Council (hereinafter, "HRC") have adopted subsequent resolutions providing guidance to states on how to better safeguard the right to privacy. Additionally, the HRC appointed a new Special Rapporteur on the right to privacy to give more focused attention to this issue.

Focus on the gendered dimensions of privacy has been relatively limited to date, but has increased in recent years. The mandate of the Special Rapporteur on the right to privacy tasks the Special Rapporteur with "integrat[ing] a gender perspective throughout the work of the mandate."[7] Additionally, HRC resolution 34/7 and the UNGA have noted that "violations and abuses of the right to privacy in the digital age may affect all individuals, including with particular effects on women, as well as children and persons in vulnerable situations, or marginalized groups,"[8]

[4]United Nations General Assembly. (2014). *The right to privacy in the digital age*, A/RES/71/199. https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/71/199
[5]United Nations High Commissioner for Human Rights (2014). *The right to privacy in the digital age*, A/HRC/27/37.https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf
[6]United Nations High Commissioner for Human Rights. (2018). *The right to privacy in the digital age*, A/HRC/39/29. https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/A_HRC_39_29_EN.docx
[7]Human Rights Council. (2015). *The right to privacy in digital age*, A/HRC/RES/28/16. p.4 (OP 4f) https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/28/16
[8]Human Rights Council. (2017). *The right to privacy in the digital age*, A/HRC/RES/34/7, p. 4. https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/34/7

and called on states "to further develop or maintain, in this regard, preventive measures and remedies for violations and abuses regarding the right to privacy in the digital age that may affect all individuals, including where there are particular effects for women, as well as children and persons in vulnerable situations or marginalized groups."[9]

Additionally, the HRC's resolution on "accelerating efforts to eliminate violence against women and girls: preventing and responding to violence against women (hereinafter, "VAW") and girls in digital contexts" noted that all forms of discrimination, intimidation or harassment and violence in digital contexts prevent women from fully enjoying their human rights, including the right to privacy.[10] The resolution goes on to recognise not only that technologies can offer access to information and enable women to make autonomous decisions regarding their own bodies, lives or health, but also that "encryption and anonymity may contribute to individuals' full enjoyment of human rights, including the right to freedom of opinion and expression and the right to privacy" and may empower women "to access information and ideas, to seek help, assistance and guidance and to freely explore and express ideas relating to their identity and human rights."[11]

The Special Rapporteur on VAW, its causes and consequences dedicated her 2018 report to "online violence against women and girls from a human rights perspective",[12] which included a section on "the right to live free from gender-based violence and the right to privacy and data protection". The report outlined the many forms of online gender-based violence that violate women's and girls' rights to privacy. It noted, for example, that "the publication or posting online without consent of intimate photographs or photoshopped images that are sexualized or have been created to humiliate, shame or stigmatize a woman is a violation of a woman's right to dignity and to live a life free from violence."[13] The report also highlighted the important role of anonymity online for women and others at risk of discrimination and stigma; for example, it allows them to seek information, find solidarity and support and share opinions without fear of being identified. Echoing an earlier report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,[14] the report noted that this holds

[9]Ibid.
[10]Human Rights Council. (2018). *Accelerating efforts to eliminate violence against women and girls: preventing and responding to violence against women and girls in digital contexts*, A/HRC/38/5. https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/38/5
[11]Ibid.
[12]Simonovic, D. (2018). *Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective*, A/HRC/38/47. https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session38/Documents/A_HRC_38_47_EN.docx
[13]Ibid.
[14]Kaye, D. (2015). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/29/32.

particularly true for individuals who face discrimination and persecution based on their sexual orientation and gender identity. The Special Rapporteur on VAW recommended that states should ensure that their legal frameworks adequately protect all women's human rights online, including the right to privacy and data protection, and that they should should protect and encourage the development of encryption and anonymity tools that protect the rights and security of women online.

Finally, in 2017, a group of international human rights experts and advocates developed the Additional Principles and State Obligations on the Application of International Human Rights Law in Relation to Sexual Orientation, Gender Identity, Gender Expression and Sex Characteristics to Complement the Yogyakarta Principles, known as the Yogyakarta Principles Plus 10 (YP+10).[15] The YP+10 document was developed to reflect both developments in international human rights law and the emerging understanding of violations suffered by persons on grounds of sexual orientation and gender identity and the recognition of the distinct and intersectional grounds of gender expression and sex characteristics. Notably, it included a new Principle (36) on "the right to the enjoyment of human rights in relation to information and communication technologies",[16] which included the following state obligations:

> D. Respect and protect the privacy and security of digital communications, including the use by individuals of encryption, pseudonyms and anonymity technology;
> E. Ensure that any restrictions on the right to privacy, including through mass or targeted surveillance, requests for access to personal data, or through limitations on the use of encryption, pseudonymity and anonymity tools, are on a case specific basis, and are reasonable, necessary and proportionate as required by the law for a legitimate purpose and ordered by a court;
> F. Take measures to ensure that the processing of personal data for individual profiling is consistent with relevant human rights standards including personal data protection and does not lead to discrimination, including on the grounds of sexual orientation, gender identity, gender expression and sex characteristics.

https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc

[15]Additional Principles and State Obligations on the Application of International Human Rights Law in Relation to Sexual Orientation, Gender Identity, Gender Expression and Sex Characteristics to Complement the Yogyakarta Principles: https://yogyakartaprinciples.org/principles-en/yp10

[16]Principle 36 "The Right to the Enjoyment of Human Rights in Relation to Information and Communication Technologies": https://yogyakartaprinciples.org/principle-36-yp10

The YP+10 document also outlined additional state obligations regarding the principle on the right to privacy (Principle 6).[17]

3. A gendered understanding of privacy

> *"If we agree that the online world is socially constructed, then gender norms, stereotypes and inequality that exist offline [...] can be replicated online."*[18]

An offline world with misogyny, heteropatriarchal heritage and gendered injustices is not only replicated online, but can also be exacerbated and take on new forms. In attempting to advance a gendered understanding of privacy, it is necessary to "adjust the lens of gender and human rights that we apply offline to enable us to map and claim our rights"[19] in the digital world. That means not only incorporating strategies and policies from the offline world, but also imagining, observing and building digital contexts with greater gender equality and women's rights.

In light of the above, we welcome the Special Rapporteur on the right to privacy's consultation on "gender perspectives on privacy", because – as we repeatedly emphasise in this report – violations related to surveillance, privacy and personal data are not gender-neutral. This makes it crucial to adopt a gendered perspective to comprehensively analyse the particular harms to the right to privacy that affect women and the LGBTIQ population. This section will specifically focus on (3.1) a better understanding of privacy and how the right to privacy is crucial for the development of sexual and gender identities; (3.2) issues of security and surveillance, and how both state and non-state surveillance, including surveillance among peers, have particular impacts on women and LGBTIQ people; and (3.3) the use of personal data by corporations and the need to incorporate a gender lens in companies' business models.

3.1. A better understanding of privacy

In addition to being a fundamental right in and of itself, privacy provides a safe sphere to engage in self-development without concern for being misunderstood or judged, and enables intimate relationships, which are essential for the development of one's personality[20] as well as the construction of one's own specific identity. Numerous sexuality-related decisions regarding one's private life, including the

[17]Original Principle 6: https://yogyakartaprinciples.org/principle-6 and Additional state obligations for Principle 6: https://yogyakartaprinciples.org/relating-to-the-right-to-privacy-principle-6
[18]Fascendini, F., & Fialová, K. (2011). *Voices from Digital Spaces: Technology-related violence against women*. APC. https://www.genderit.org/node/3539
[19]Sandler, J. (2013). Introduction. In Finlay, A. (Ed.), *Global Information Society Watch 2013: Women's rights, gender and ICTs*. APC and Hivos. https://www.giswatch.org/sites/default/files/introduction_gisw13.pdf#6
[20]Keats Citron, D. (2018). Sexual Privacy. *Yale Law Journal,* Forthcoming. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3233805

choice of intimate partners or whether to terminate a pregnancy, occur in private spheres,[21] and these decisions play an important role in the development social identity. When such decisions are interfered with and/or when individuals lose control over their personal information, the result is not just a privacy harm but also a harm to their identity. Control over one's personal information is, therefore, not only important for respecting their right to privacy, but also their ability to manage intimate relationships and other aspects of their personal lives intrinsic to the development of personality.

Anonymity and encryption "provide a 'zone of privacy' within which one can exercise their freedom of expression and opinion."[22] Anonymity makes it possible to control what personal information is shared and how that information can be used. Anonymity online enables individuals and minority groups to associate on sensitive matters, including sexual orientation.[23] It creates enabling environments for people to share and seek sensitive information and engage in online associations based on identities which can be illegal in some countries, such as people who identify as LGBTIQ. Marginalised or persecuted sexual minorities find spaces for exercising their freedom of speech and association more privately in online spaces as compared to offline spaces, and it is therefore crucial that they have access to tools that enable them to protect the confidentiality of digital communications to ensure their enjoyment of human rights.

The Special Rapporteurs on freedom of opinion and expression and on violence against Women have both highlighted in their reports the importance of encryption and anonymity online for women and others at risk of discrimination and stigma, in that it allows them to seek information, find solidarity and support and share opinions without fear of being identified. This holds particularly true for individuals who face discrimination and persecution based on their sexual orientation and gender identity.[24]

A clear example of the aforementioned are the findings of the global survey conducted by APC as part of the EROTICS (Exploratory Research on Sexuality and the Internet)[25] project. It revealed that "the internet is considered an 'important' or 'very important' medium of sexual expression by 66% of the sample (among them,

[21]Ibid.
[22] Van der Spuy, A., & Aavriti, N. (2018). *Mapping research in gender and digital technology.* APC. https://www.apc.org/sites/default/files/IDRC_Mapping_0323_0.pdf
[23]APC. (2015). *The right to freedom of expression and the use of encryption and anonymity in digital communications: Submission to the United Nations Special Rapporteur on the right to freedom of opinion and expression.* https://www.apc.org/sites/default/files/APC%20submission%20to%20SR%20FOEX_20150211_0.pdf
[24]A/HRC/29/32 and A/HRC/38/47. Op. cit.
[25]EROTICS is a network of activists and researchers working at the intersections of sexuality and the internet. More information at: https://erotics.apc.org/about-erotics

39% consider it 'very important')."[26] However, while the internet is an essential tool to communicate and spread critical information regarding LGBTIQ activism, these activists also face significant threats online: "the most frequent is harassment (75%), followed by intimidating online comments (63%) and blocked websites or filtering software that prevented the user from accessing information (54%)."[27].

It is also relevant to highlight the importance of privacy in dating apps, especially for LGBTIQ population. Dating apps provide a unique space to communicate within a safe community without the persecution or stigma that may be experienced in other dating methods. However, design choices, as well as terms and conditions of use, impact how safe and secure such apps are. For example, in Egypt dating apps have been used to identify and prosecute homosexual people, and in several countries to disclose non-consensual intimate images for the purposes of extortion.[28] The Egyptian police used dating apps to identify and entrap LGBTIQ people to accuse them of "promoting sexual deviancy" or "habitual debauchery charges".[29] Research by ARTICLE 19 revealed that persecution through dating apps is a tendency not only in Egypt but also in Lebanon and Iran; in addition, non-state actors in those countries use fake accounts to blackmail individuals for money or for sexual services or cruel and degrading treatment.[30] According to the ARTICLE 19 report, "Blackmail seems more prevalent through dating-specifics apps in Egypt and Lebanon, while in Iran these cases occur via messaging apps such as Telegram."[31] The report also revealed the criminalisation of the use of these apps: the existence of an app logo on a mobile phone alone could be sufficient grounds for arrest or prosecution. "The sole issue of having the apps puts you in a vulnerable situation," an anonymous app user reported.[32]

It is therefore critical for developers of these apps to engage in conversations with the people and communities that use them, ideally to design the apps *with* rather than *for* them, in order to enable technical solutions to secure and protect confidentiality as a means to protect freedom of expression and gender identities in

[26]Vale, H. (2018). *Body as data: EROTICS exploratory research on sexuality, rights and the internet*. https://slides.com/hvale/body-as-data-dataveillance-the-informatisation-of-the-body-and-citizenship#/1
[27]APC. (2017). *EROTICS Global Survey 2017: Sexuality, rights and internet regulations*. https://www.apc.org/sites/default/files/Erotics_2_FIND-2.pdf
[28]For more information see Malhotra, N. (2015). *Good questions on technology-related violence*. APC. https://www.apc.org/en/pubs/good-questions-technology-related-violence, https://acoso.online and Tyler, J. (2016, 26 August). Jilted Tinder lover threatened student with revenge porn and bombarded her with texts begging for sex. *Mirror.* https://www.mirror.co.uk/news/uk-news/jilted-tinder-lover-threatened-student-8714478
[29]Young, L. (2017, 4 October). Egyptian police using dating apps to find, arrest gay people in new crackdown. *Global News.* https://globalnews.ca/news/3784780/egypt-gay-crackdown-dating-app
[30]ARTICLE 19. (2018). *Apps, arrests and abuse in Egypt, Lebanon and Iran.* https://www.article19.org/wp-content/uploads/2018/02/LGBTQ-Apps-Arrest-and-Abuse-report_22.2.18.pdf
[31]Ibid.
[32]Ibid.

digital contexts. In this vein, it is also critical that states do not interfere with the availability or use of encryption or impose restrictions in contravention of international human rights law because of the importance of anonymity for persons who face discrimination based on their gender, sexual orientation, or gender identity and expression.

Mobile phones offer a good example of how privacy, technology and the internet can enhance the autonomy and personality development of young women, and how gender-biased efforts to restrict their use can diminish women's autonomy. In Northern India, the use of mobile phones, and specifically apps like WhatsApp and Facebook, by women and girls under 18 prompted political leaders in their villages to ban their use. The connectivity and relative privacy that mobile phones afforded make women and girls more independent; they can experience love and affection on their own terms and make transactions on their own behalf, increasing their individual choices.[33] The new ideas of self and the creation of new spheres of privacy that were not available before to young women in these communities enabled by mobile phones have disrupted the existing patriarchal regime of control and surveillance that ruled in these Indian villages. Despite the Indian Supreme Court's criticism of this form of surveillance, the mobile phone bans are still in place and serve a desire to control women's behaviours including their conversations, actions, choices and movements.

3.2. Security and surveillance

Surveillance serves as a tool of social control, defining who is within the norm and who is outside of it.[34] From a gendered perspective, we see three overlapping dimensions of surveillance:

- Body discrimination: Technologies are not designed to understand different types of bodies, and so they privilege certain bodies – usually male, young and white – over others. That creates a tool of discrimination against everyone who does not fit it, treating them as deviant. A clear example of this is the whole-body imaging technologies that are used in many airports to screen passengers. Despite their seemingly being objective and neutral, these technologies discriminate against bodies that are not privileged, which means some people are far more likely to be treated as a potential threat, and thus to be singled out for secondary screening, than those with "normative" body types. Those whose body types may therefore render them "deviant" include obese people, who supposedly could hide weapons.[35]

[33]Kovacs, A. (2017a). Chupke, Chupke: Going Behind the Mobile Phone Bans in North India. *Gendering Surveillance.* https://genderingsurveillance.internetdemocracy.in/phone_ban
[34]Shephard, N. (2016). *Big Data and Sexual Surveillance*. Association for Progressive Communications. https://www.apc.org/sites/default/files/BigDataSexualSurveillance_0_0.pdf

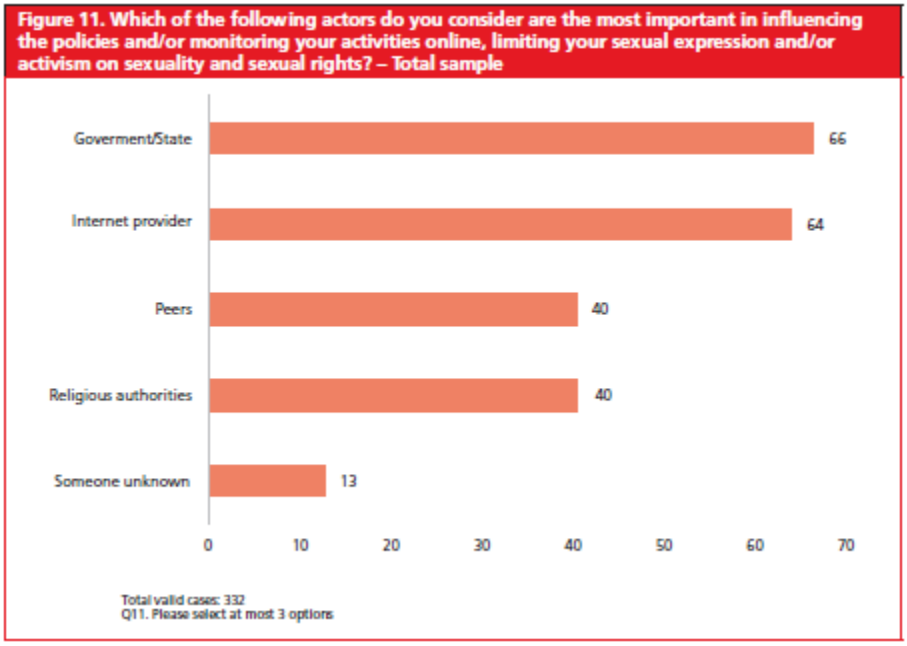
- Context or use discrimination: When contexts are already marked by sexist relations and patriarchal structures, surveillance tends to amplify those tensions and inequalities, reproducing inequalities.[36] Returning to the example of whole body imaging technologies, transgender people are at a heightened risk of being treated as "deviant" and subjected to additional screenings.[37]
- Discrimination by abstraction: Data is the key element of surveillance in the digital era, and when people are reduced to data points in databases, disembodied from social context, abstract representations of the world such as social inequalities are not adequately reflected in the data and are thus rendered invisible.[38]

Women's privacy experiences differ from those of men in large part because women are more exposed to lateral surveillance. This kind of surveillance, carried out by peers like family members, friends or acquaintances, can consist of stalking someone's online presence by collecting details of their personal lives through search engines, following their social media presence, and posting excessive and/or threatening comments online.[39] If the context is already patriarchal or abusive, this can be extended and even exacerbated in the digital context, affecting women's freedom of expression and right to privacy.

Women may be targeted by actions that comprise both gender-based violence and infringement of privacy, such as accessing, using, manipulating or disseminating private data without consent; contacting or harassing women's children, colleagues or family to gain access to them; or using spyware or keystroke loggers to monitor them. These forms of surveillance and monitoring are not only conducted by state authorities but also by non-state actors. While, as noted in the previous section, mobile phones can help to expand the physical spaces and opportunities in which women can engage, this potential is curbed by surveillance on the part of such actors as the nuclear family, universities or employers.[40]

According to APC's 2017 EROTICS Global Survey, 40% of respondents said that peers or people that they know are the actors who most frequently monitor their online activities, limiting their sexual expression and/or activism on sexuality and sexual rights.[41] This reveals the size of lateral surveillance in digital contexts and how it works as an inhibitor of activism.

[35]Kovacs, A. (2017b). Reading Surveillance through a Gendered Lens: Some Theory. *Gendering Surveillance*. https://genderingsurveillance.internetdemocracy.in/theory
[36]Monahan, T. (2009). Dreams of Control at a Distance: Gender, Surveillance, and Social Control. *Cultural Studies <-> Critical Methodologies, 9*(2), 286-305.
[37]Kovacs, A. (2017b). Op. cit.
[38]Ibid.
[39]Shephard, N. (2016). Op. cit.
[40]Kovacs, A. (2017a). Op. cit.
[41]APC. (2017). Op. cit.



According to the same survey, social media is the most frequent situation in which surveillance is experienced, and 43% of the respondents suffered at least one instance of being intensively follow by other people on social media. In second place, 39% of the respondents indicated that someone attempted to obtain their username, password and credit card details, and this is closely followed by 38% who said that mainstream apps had used their location data and/or personal information without their knowledge or consent.[42] A gender and sexual orientation bias is evident in the higher surveillance percentages of respondents who self-identified as LGBQ: 47% said they have been followed on social media versus 37% of heterosexuals, and 43% said that someone attempted to obtain their username, password and/or credit card details versus 31% of heterosexuals.[43]

[42]Ibid.
[43]Ibid.

Table 4. Have you ever experienced any of the following situations regarding surveillance? – By sexual orientation		
Situation of surveillance	LGBQ	Heterosexual
Following on social media	47%	37%
Passwords	43%	31%
Use of your personal information	39%	32%
Photographed or filmed	35%	29%
Screening	29%	23%
Tracking app	21%	14%
Wiretapped	13%	6%
Q13. Choose one option per row		

Digital voyeurism is enabled by numerous technological devices that can be used to spy on women in private places, such as cell phone cameras or smart-home technologies. Cyberstalking apps enable monitoring of what people are doing in their homes, their movements and communications. It is common for men to violate their female partners' privacy through tracking and controlling using GPS and spyware devices. Even location data or sleep monitoring apps that are not designed for this purpose work as lateral surveillance tools as well. With the rise of the internet of things (IoT), new opportunities to violate the right to privacy have also emerged.[44] Smart-home technologies in particular have been shown to facilitate new forms of domestic violence through new ways to harass, to monitor, to take control inside the household. A clear example is how in an abusive relationship, a husband can monitor if his wife is in their bedroom or not and if she is alone or not, and record her movements by video, among others. The majority of victims in these types of cases are women, which reveals an asymmetry of power, because their partners have the control and power of technology.[45] This is consistent with what the Special Rapporteur on the right to privacy observed in his 2018 report to the HRC, specifically that domestic violence can be enabled by digital devices.[46]

3.3. Use of personal data by corporations

The business model adopted by many corporations relies on the exploitation of personal data of users. Personal data is a key element for the displaying targeted advertisements in online contexts (also known as behavioural advertising). To do

[44]Bowles, N. (2018, 23 June). Thermostats, Locks and Lights: Digital Tools of Domestic Abuse. *The New York Times*. https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html
[45]Ibid.
[46]Cannataci, J. (2018). *Report of the Special Rapporteur on the right to privacy,* A/HRC/37/62. https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session37/Documents/A_HRC_37_62_EN.docx

this, it is necessary to collect, recombine and analyse all kinds of personal data and metadata to profile future customers and sell this information to advertisers. Retail information, health records, work records, police records and others are useful data to profile and sell to advertising companies. Privacy harms can originate in business models, which makes it crucial to increase transparency on how private companies are using sensitive data. Platforms have a responsibility to inform users of their specific risks and create features that can mitigate those risks.

Data processing never takes place in a gender-neutral manner, and the practices of such companies are no exception. A clear example is the recording, tracking and gathering of data on sexual and reproductive behaviours by corporations through period tracking apps. Although these apps may portray themselves as positive services, they are also new models of surveillance – self-surveillance – and thereby new models to define what is within the norm and what is not. As the NGO Coding Rights has observed, these apps are ruled by a particular world view, normally run by men, with a particular vision of what women's role is, and "these men and their world view define the terms around what will be measured and why and whom will be measured and how."[47] Thus, the data gathered and share with third parties may generate algorithms with the potential to create "new standards for reproductive and gynaecological indicators based only on those women who have access to these apps, and those who bother to use them."[48] These mechanisms may give rise to the formation of new normative ideas around health and reproduction that affect women's bodies.

A clear example of how the use of personal data by companies can result in privacy harms is the case of Grindr and its data-sharing practices. In February 2018, the Swedish public broadcaster SVT and the Norwegian research institute SINTEF conducted an experiment to analyse privacy leaks in the dating application Grindr. They discovered that Grindr contains many trackers and shares personal information with various third parties directly from the app, including users' HIV status.[49] Another example is the ability of apps to monitor, localise and even send specific propaganda to women and girls who are in the process of obtaining an abortion, either undergoing an abortion, considering it, or even when they are in the clinic waiting room.[50] This not only presents a serious privacy and security

[47]Felizi, N., & Varon, J. (2016). Menstruapps – How to turn your period into money (for others). *Chupadados.* https://chupadados.codingrights.org/en/menstruapps-como-transformar-sua-menstruacao-em-dinheiro-para-os-outros
[48]Rizk, V., & Othman, D. (2016). Quantifying Fertility and Reproduction through Mobile Apps: A Critical Overview. *ARROW for Change, 22*(1). https://www.arrow.org.my/wp-content/uploads/2016/08/AFC22.1-2016.pdf
[49]Belluz, J. (2018, 3 April). Grindr is revealing its users' HIV status to third-party companies. *Vox.* www.vox.com/2018/4/2/17189078/grindr-hiv-status-data-sharing-privacy; more information at: github.com/SINTEF-9012/grindr-privacy-leaks
[50]Coutts, S. (2016, 25 May). Anti-Choice Groups Use Smartphone Surveillance to Target 'Abortion-Minded Women' During Clinic Visits. *Rewire News*. https://rewire.news/article/2016/05/25/anti-

threat to women but also a shameless violation of their sexual and reproductive health rights.

To combat the privacy harms experienced as a result of the use of personal data, consent is key, specifically, free, prior, meaningful and informed consent. Social media platforms and dating apps should embed users' consent into the user experience (UX) design and algorithms of their code. Most developers are not prioritising consent. Quite to the contrary, the dominant priority on the internet today is to extract as much data as possible with little attention to who is posting data about whom, guided by opaque and difficult to understand terms of service. For instance, Facebook is the most used social network to express critical opinions, share information and carry out activism. At the same time, according to the 2017 EROTICS Global Survey, 55% of respondents perceived Facebook as the most dangerous platform, because they believe it has access to a lot of personal information, and the privacy terms are not transparent, are constantly changing, and it is well known that Facebook sells personal information to governments and companies for marketing, publicity or political reasons.[51] Another relevant case is Facebook's real-name policy, which not only dangerously exposes transgender people, activists and survivors of domestic violence to multiple threats (psychological, physical and financial), but also contributes to unequal treatment and protection of members of the LGTBIQ population whose "legal names" do not accord with their gender identity.[52] In light of the aforementioned, it urgent to make terms and conditions more transparent and respect the rights of all users, including people with diverse sexual orientations and gender identities and expressions.

4. New or significantly different gender-based experiences of privacy in the digital era

Gendered experiences of privacy in the digital area are rooted in hetero-patriarchal social and cultural norms. As the HRC has recognised, violence against women and girls, including privacy violations occurring in digital contexts, is a "phenomenon rooted in historical and structural inequalities in power relations between women and men, which further reinforce gender stereotypes and barriers to women's and girls' full enjoyment of all human rights."[53] The digital era has produced some new and different gender-based experiences of privacy, a few examples of which are detailed below. However, it is important to keep in mind that there is a continuum between online and offline realities, and privacy violations enabled by digital

choice-groups-deploy-smartphone-surveillance-target-abortion-minded-women-clinic-visits
[51]APC (2017), EROTICS. Op. cit. p. 27
[52]Goldsman, F. (2014, 5 October). *Facebook: The king laid bare and the drag queens. APC*. https://www.apc.org/en/blog/facebook-king-laid-bare-and-drag-queens and Nameless Coalition. (2015, 5 October). Open letter to Facebook on real name policy. *APC*. https://www.apc.org/en/node/21119
[53]A/HRC/RES/38/5. Op. cit.

technologies impact people's offline, lived realities. It is also key to consider that different experiences of privacy on the basis of gender are a result both of the fact that people are the target of privacy violations and abuses because of their gender, sexual orientation or gender identity or expression, and because "gender-neutral" privacy violations (like data breaches) can have a more severe impact on women and LGBTIQ people due to historical and structural inequalities in power relations between women and men.

4.1. Privacy violations as a facet of online gender-based violence

As noted above, women and girls face specific threats to their privacy in the digital age, including cyberstalking, exposure of personal information, manipulation of images, and non-consensual distribution of intimate images or distribution "sex videos"[54] that are used for blackmail and can result in repeated trauma every time they are re-posted online.[55] While the gender-based violence (GBV) is not new, the technological dimension adds elements of searchability, persistence, replicability and scalability[56] which facilitate aggressors' access to women they are targeting and can escalate and exacerbate harm. Below we include a non-exhaustive list of forms of online GBV that constitute privacy violations:[57]

- Accessing, using, manipulating and/or disseminating private data without consent (by cracking[58]personal accounts, stealing passwords, using/stealing identities, using another person's computer to access a user's accounts while it is logged in, etc.).
- Taking, accessing, using, manipulating, and/or disseminating photographs and/or videos without consent (including so-called "revenge porn").

[54]This type of violation is commonly referred to as "revenge porn", a misnomer which simultaneously applies implicit blame to the victim/survivor, ignores a full range of aggressors and invokes a moralist reaction. Citing that an action is the result of "revenge" implies that the aggressor was provoked by an inappropriate action of the victim, who was somehow responsible or could have avoided it. It further puts this type of violence into a two-person intimate partner relationship, ignoring the many motives and points of access and distribution possible, thus limiting the possibility of redress or application of sanction to others involved. Furthermore, it assumes that the material is pornographic, which is defined differently in each country's national legislation, but in theory is a specific commercial relationship based on consent, which is not reflected in the majority of cases of non-consensual distribution. Pornography and voluntary sexual content production is frequently received from a moralistic, heteronormative standpoint and those who participate in it can be subject to harsh societal judgement.

[55]Fascendini, F., & Fialova, K. (2013). Op. cit.

[56]boyd, d. (2010). Social Network Sites as Networked Publics. In Papacharissi, Z. (Ed.), *Networked Self: Identity, Community, and Culture on Social Network Sites.* www.danah.org/papers/2010/SNSasNetworkedPublics.pdf

[57]APC. (2017). *Online gender-based violence: A submission from the Association for Progressive Communications to the UN Special Rapporteur on violence against women, its causes and consequences*. https://www.apc.org/sites/default/files/APCSubmission_UNSR_VAW_GBV.pdf

[58]The term "cracking" is used rather than "hacking" to indicate a forced entry or takeover of content with malicious intent, while "hacking" could include similar actions that are bona fide and/or done in the public interest.

- Sharing and/or disseminating private information and/or content, including (sexualised) images, audio clips and/or video clips, without knowledge or consent.
- Doxing (researching and broadcasting personally identifiable information about an individual without consent, sometimes with the intention of providing access to the woman in the "real" world for harassment and/or other purposes).
- Contacting and/or harassing a user's children, extended family, colleagues, etc. to gain access to her.
- Sexualised blackmail and/or extortion.
- Theft of identity, money and/or property.
- Impersonation resulting in physical attacks.
- Monitoring, tracking and/or surveillance of online and offline activities.
- Using spyware or keystroke loggers without consent.
- Using GPS or other geolocator software to track a woman's movements without consent.

Perhaps the form of privacy-violating online GBV that is most visible is the publication or posting online without consent of intimate photographs and photoshopped images that are sexualised or have been created to humiliate, shame or stigmatise a woman, which is a violation of a woman's right to dignity and to live a life free from violence.[59] Such forms of online violence create a permanent digital record that can be distributed worldwide and cannot be easily deleted, which may result in further victimisation of the victim.[60] According to the 2018 report of the Special Rapporteur on violence against Women:

> Relevant data and surveys have shown that, in the majority of cases, online violence is not a gender-neutral crime. Surveys of the gender dimension of online violence indeed indicate that 90 per cent of those victimized by non-consensual digital distribution of intimate images are women.[61]

It is important to understand that non-consensual dissemination of intimate images can occur whether the perpetrator obtained the nude images with consent – normally in the context of an intimate relationship – but afterwards distributed them without the victim's consent, or whether the perpetrator obtained sexual images without the consent of the victim and then distributed the material. Recording sexual images and sharing them with a sexual partner is a natural manner to explore and develop sexuality and women should never be accused,

[59]A/HRC/38/47. Op. cit.
[60]Ibid.
[61]Ibid.

persecuted or misjudged because of that. However, non-consensual dissemination of intimate images, in cases where there was no consent for the recording and/or distribution of sexual images, is a violation of the right to privacy in digital contexts.

4.2. Dataveillance

Dataveillance combines data and surveillance to describe systematic data-based surveillance practices that involve sorting and aggregating large quantities of data to monitor, track and regulate people and populations.[62] Dataveillance can serve to describe behaviours (monitoring) but also to predict them (conjecture) and even prescribe them (enactment).[63] Massive personal data (and metadata) collection never takes place in a neutral manner; on the contrary, data collection always has a gender and sexual bias, creating and maintaining hetero-patriarchal dynamics in digital contexts. Dataveillance thus by definition runs the risk of reproducing past discriminations and marginalisations through new modes of algorithmic discrimination. Moreover, with big data, the possibilities of shaping people's behaviours have become ever more comprehensive.[64]

In an issue paper written for APC, *Big Data and Sexual Surveillance*, Dr. Nicole Shephard states that as public health, development, state security as well as private industries increasingly move online and embrace big data, analysing the gendered effects of the data practices involved is timely and warranted. She concludes:

> The picture that emerges on the nexus between big data and sexual surveillance is an ambiguous one. Calls for better representation of women and queers, for reaping data's benefits in terms of development, gender equality, and sexual health, and for better recognition of gender-based and sexual violence have the potential to improve the lives of marginalised groups. They, however, have to be leveraged against concerns about the politics of the collection and analysis of big data, discriminations coded into the collection and algorithmic analysis of data, its colonial legacies, and the complicated politics of visibility that go along with the presence in data.[65]

Whether data practices are transformative depends on agency and consent, on how data is collected, by whom, and to what ends. While data-driven sexual surveillance often takes place on the level of abstraction, it produces embodied consequences and meanings. Given the pervasive yet unaccountable nature of dataveillance practices, the protection of information privacy and anonymity remain a prerequisite for any transformative use of data. When developing or participating in

[62]Shephard, N. (2016). Op. cit.
[63]Ibid.
[64]Ibid.
[65]Ibid.

data practices it is essential to remain attentive to consent and participation and take adequate care to safeguard the data of vulnerable groups involved as well as of activists themselves at risk of surveillance.[66]

4.3 Digital security divide

One of the gendered impacts of privacy and, at the same time, one of the biggest challenges to the enjoyment of human rights in the digital age is the digital divide between men and women. APC understands meaningful internet access to mean pervasive, affordable connectivity (of sufficient quality and speed) to the internet in a manner that *enables the user to benefit from internet use, including to participate in the public sphere, exercise human rights, access and create relevant content, and engage with people and information for development and well-being*.[67] The gender digital divide can create a disparity in the protection of the right to privacy because of the disparity in skills between men and women to manage their data to protect their privacy online.[68] Women's ability to gain meaningful internet access is influenced by factors including location, economic power, age, gender, racial or ethnic origin, social and cultural norms, and education, amongst other things.[69] Disparity and discrimination in these areas translate into specific gender-based challenges and barriers to meaningful access. For example, gender literacy gaps – including digital literacy – result in uneven capacity among women to use the internet for their needs, including to protect their privacy online.[70] Thus, bridging gender digital divides and increasing women's capacities to identify and manage data and surveillance practices by learning about privacy, safety and encryption mechanisms should be supported and amplified.[71] Indeed, this is one of the most important challenges to be addressed to reduce gendered privacy risks.

4.4 Data breaches

As noted earlier, data collection never takes place in a gender-neutral setting, so when data breaches occur, even if they are not targeting people specifically on the basis of gender, they can have a more severe impact on women and LGBTIQ people

[66]Ibid.
[67]APC. (2017b). *Bridging the gender divide from human rights perspective: APC submission to the Office of the High Commissioner for Human Rights*. https://www.apc.org/sites/default/files/APCSubmission_OHCHR_BridgingGenderDigitalDivideHumanRightsPerspective_0.pdf
[68]Park, Y. J. (2015). Do men and women differ in privacy? Gendered privacy and (in)equality in the Internet. *Computers in Human Behavior, 50*. https://www.researchgate.net/publication/275365626_Do_men_and_women_differ_in_privacy_Gendered_privacy_and_inequality_in_the_Internet
[69]Milek, A., Stork, C., & Gillwald, A. (2011). Engendering communication: A perspective on ICT access and usage in Africa. *Info: The Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media, 13*(3), 125-141.
[70]APC. (2017b). Op. cit.
[71]Van der Spuy, A., & Aavriti, N. (2018). Op. cit.

because of historical and structural inequalities in power relations between women and men.

For example, on July 2016, the municipality of São Paulo experienced a data breach exposing the personal data of an estimated of 650,000 patients from the Brazilian public health system. This massive data breach included names, addresses and medical information such as abortion cases and pregnancy stages.[72] According to the media, the personal data was from 2001 to 2007 and referred – in almost of all of the cases – to women in some point of their pregnancy. Among those affected were 15,926 mothers who had given birth before seven months of gestation, 4,237 abortions and 181 recent stillbirths. It is worth noting that abortion is illegal in Brazil, so this data breach not only violated the right to privacy of the women affected around a socially sensitive issue, but also exposed them and their doctors to potential criminal charges.

The aforementioned example constitutes a clear example that personal data breaches can dramatically affect not only women's privacy but also their sexual and reproductive health rights, their dignity and self-development. When data breaches occur it is crucial to observe with a gender lens which human rights can be affected and analyse beyond privacy frames; in this case, a hospital is a critical infrastructure (because of the management of sensitive and health data) that should have heavy security measures as part of a cybersecurity policy respectful of human rights. This highlights a key point, the need for countries to implement cybersecurity policies with a human rights perspective.

Another massive data breach occurred in Chile in 2016. In this case, a public hospital suffered a cybersecurity failure and made available to their workers and even to the general public (via their intranet) more than three million health records including the names, ID numbers and addresses of women and girls who asked for the morning-after pill in a public hospital and people living with HIV.[73] The authorities had been alerted to this flaw in the hospital's computer system 10 months earlier, but neither the authorities nor the company in charge of the hospital's cybersecurity took action to remedy the situation despite being warned of the risks.[74] The people most affected by the data breach were women, girls and people living with HIV. Women and sexual minorities are more profoundly affected by the consequences of these kinds of data breaches because they impact on not only their right to privacy but also their sexual and reproductive health and rights.

[72]Hernandes, R. (2016, 6 July). Gestão Haddad expõe na internet dados de pacientes da rede pública. *Folha de Sao Paulo*. https://www1.folha.uol.com.br/cotidiano/2016/07/1788979-gestao-haddad-expoe-na-internet-dados-de-pacientes-da-rede-publica.shtml
[73]Jara, M., & Carvajal, V. (2016, 3 March). Grave falla en la red del Minsal dejó expuesta información confidencial de pacientes. *CIPER*. https://ciperchile.cl/2016/03/05/grave-falla-en-la-red-del-minsal-dejo-expuesta-informacion-confidencial-de-pacientes
[74]Ibid.

5. Gendered impacts of privacy invasions on women, men and individuals of diverse sexual orientations gender identities, gender expressions and sex characteristics, arising from the loss of the right to privacy

Based on analysis of 1,126 cases reported via the Take Back the Tech! online mapping platform and 24 in-depth case studies,[75] we can share the following observations about the gendered impact of privacy invasions on women arising from the loss of the right to privacy due to online GBV:

- ***Social isolation*** through which victims/survivors withdrew from public life, including with family and friends. This was particularly true for women whose photos and videos were distributed without their consent and who felt publicly humiliated and ridiculed. As shared in a case study: "I felt like I lost something, perhaps my confidence. For one year, I did not talk to people. I felt there was nothing for me to say so I did not talk."[76]
- ***Economic loss*** through which victims/survivors became unemployed and lost income. For example, Ruby[77] was forced to resign from her job after sex videos were distributed online without her consent. She said: "I had been working for [only] five years and I did not expect to lose my job. All my contracts ended at the same time, just when the scandal erupted."[78]
- ***Psychological harm*** through which victims/survivors experience depression, anxiety and fear. There was also a certain point where some victims/survivors expressed suicidal thoughts as a result of the harm they faced. One woman recounts, "I considered committing suicide, because I figured that this would send the message that this wasn't a game."[79]
- ***Self-censorship*** for fear of further victimisation and due to loss of trust in the safety of using digital technologies, which was the case of Alejandra, who completely withdrew from the internet for a long period of time.[80] Removing oneself from the internet has further implications beyond self-censorship, such as access to information, e-services, and social or professional communication.
- ***Limited mobility*** through which victims/survivors lost the ability to move around freely and participate in online and/or offline spaces. In one case, the survivor's education came to an end because her father believed it was her

[75]See www.genderit.org/onlinevaw/countries
[76]Foundation for Media Alternatives. (2014). *Case study number 2, the Philippines*. APC. https://www.genderit.org/sites/default/files/case_studies_phil3_1_0.pdf
[77]Name changed to protect victim's identity.
[78]Foundation for Media Alternatives. (2014). Op. cit.
[79]Si Jeunesse, S. (2015). *Case study number 1, Democratic Republic of Congo*. APC. https://www.genderit.org/sites/default/files/case_studies_rdc1_2_0.pdf
[80]Colnodo. (2014). *Case study number 3, Colombia*. APC. https://www.genderit.org/sites/default/files/case_studies_col3_1_1.pdf

freedom to commute to school that had ultimately led to the violence – and by extension, the "shame" suffered by the family.[81]

6. Recommendations

APC encourages the Special Rapporteur to involve organisations working on women's rights and sexual and reproductive health and rights in the work of the mandate to develop a deeper understanding of how the privacy violations they experience and their impacts their lives and communities. Additionally, we offer the following recommendations for the Special Rapporteur's consideration.

6.1 Recommendations to states

- Adopt an intersectional approach to understanding and protecting the right to privacy, which recognises the specific experiences and threats to privacy experienced by women and LGBTIQ persons.
- Enhance efforts to promote meaningful internet access, underlining the need to bridge any digital divides between women and men, including through building digital skills, as a means to contribute to protecting against privacy violations of women and LGBTIQ persons in digital contexts.
- Adopt policies, legal and regulatory frameworks that provide comprehensive protection for the use and development of secure digital communications, including by promoting strong encryption and anonymity-enhancing tools, products and services.
- Review and strengthen policies, legal and regulatory frameworks to address gender-based violence violence in digital contexts, particularly privacy violations, and ensure that all responses are in compliance with international human rights obligations, avoiding criminalisation of speech or censorship of women's sexual expression.
- Make gender a key consideration of the development and enforcement of data protection frameworks. Data protection requirements around purpose limitation, free, explicit, prior and informed consent for data processing, data minimisation, and integrity and confidentiality of data are even more critical for people who face lateral surveillance and for whom the exploitation of their data can have more severe implications for their rights to privacy, security and other fundamental rights. The right of a data subject to rectify data to ensure that is accurate, complete and kept up-to-date can have a significant impact on the rights of a transgender person, which is not typically part of debates on data protection. The risk of processing of personal data for

[81]Bukhari, G. (2014). *Case study number 3, Pakistan*. APC. https://www.genderit.org/sites/default/files/case_studies_pak1_1_0.pdf

individual profiling leading to discrimination on the grounds of sexual orientation, gender identity, gender expression and sex characteristics is only growing as digital identity programmes are becoming mandatory in many parts of the world. Such considerations must be fore-fronted to safeguard the rights of women and LGBTIQ persons in the digital age.

- Proactively involve more women and LGBTIQ persons in the design, development and regulation of digital technologies: Reversing individual and collective attitudes that perpetuate patriarchal control and abuse of personal data and violations of the right to privacy on the basis of gender requires involving more women and LGBTIQ people in the design, development and regulation of digital technologies. This is not simply a matter of representation; having a more diverse and inclusive range of people contributing to the design, development and regulation of the technologies will mean that questions, concerns and considerations about the implications of privacy on these individuals and groups will arise as well as solutions to safeguard their privacy (rather than overlook or dismiss such concerns). Promoting greater gender diversity among the people shaping online experiences decision is a shared responsibility of the state and the private sector.

6.2 Recommendations to technology companies

- Live up to their responsibilities under the UN Guiding Principles on Business and Human Rights to respect the human rights of all persons effected by their practices. This require conducting due diligence to prevent and human rights violations, mitigating adverse effects, and providing access to remedy for all persons who experienced privacy violations, bearing in mind the different risks that may be faced on the basis of gender.
- Adopt and implement privacy by design/default, while applying a gendered analysis: In addition to complying with data protection frameworks, technology companies should limit data collection to restrict further data processing, to prevent unnecessary access to and exploitation of data by utilising technological means and considering privacy in the design of systems. A key component of this is privacy by default, i.e. without requiring any action by the end-user. As the collection and processing of data is never gender neutral, it is necessary to acknowledge, recognise and address how products (such as IoT and smart-home devices) or apps (such as pregnancy or dating apps, or any location tracking app) can be exploited and violate the rights of women and LGBTIQ persons. In light of this, it is absolutely fundamental to consider gendered harms in the technical and organisational procedures of the technologies that companies create.

- Meaningfully engage with women and LGBTIQ persons in the design and development of policies and features, including by employing them as engineers and in their policy teams. Design *with* rather than *for* these individuals and groups.
- Allow for the use pseudonyms, which can help to enable the expression of diverse sexual and/or gender identities, and at the same time, help individuals to escape abusive partners, stalkers, repeat harassers and accounts associated with the sharing of non-consensual dissemination of intimate images.
- Work towards enabling technical solutions to secure and protect the confidentiality of digital communications, including measures for encryption and anonymity, and resist requests for user data that do not comply international human rights standards.
- Embed users' consent into policies and user experience design.
- Meaningfully engage in consultation with women and LGBTIQ persons, either by soliciting the input of users or by engaging women’s rights and LGBTIQ rights groups and activists, to understand the potential adverse impacts of the company's services on women’s and LGBTIQ rights