CYBER HARASSMENT HELPLINE

DECEMBER '16 - NOVEMBER '18

TWO YEAR REPORT

0800-39393

EVERYDAY 9 AM - 5 PM

Digital Rights Foundation

"KNOW YOUR RIGHTS"

About Us

Digital Rights Foundation (DRF) is a feminist, not for profit organization based in Pakistan working on digital freedom. DRF envisions a place where all people, especially women, can exercise their right of expression without being threatened.

Digital Rights Foundation believes that a free internet with access to information and impeccable privacy policies can encourage such a healthy and productive environment that would eventually help not only women but the world at large.

Acknowledgments

We can hardly believe that the helpline has been able to sustain itself for two years. What was once just a pipe dream is now an institution. This report is dedicated to our supporters and champions since day one - Urgent Action Fund, Digital Defenders Partnership, Minister of Foreign Affairs of the Netherlands and UN Women.

Of course, our real champions are our callers who place their trust in us and have allowed us to learn and evolve.

Contents

The Helpline: Our Story

Digital Rights Foundation started the Hamara Internet project in 2016. Through the project we traveled to colleges and universities across Pakistan to create awareness about digital security and online harassment among young women. Soon after the sessions, women started to reach out to us through word of mouth - our inbox was teeming with cases of women looking for advice and assistance in cases of online harassment. Given that there was no dedicated service delivery channel, the small team at Digital Rights Foundation (DRF) was unable to answer all the queries effectively, some cases started to slip through the cracks.

In the summer of 2016, online harassment and abuse in the wake of Qandeel Baloch's brutal murder saw several feminists being bullied and attacked online for their stances. Gender-based online violence was emerging as a systematic trend all over the world, and Pakistan was no exception.

Serendipity would have it that Nighat Dad, Executive Director of Digital Rights Foundation, was nominated for the Dutch Human Rights Award in August 2016. Seizing the moment, we launched an online campaign to mobilize votes with the aim of starting the region's first helpline to online harassment from the proceeds of the award. There was immense public support for Nighat's nomination, and in December 2016 as Nighat received the Dutch Tulip Award in the Netherlands, the cyber harassment helpline heard its first call back in Lahore.

Since 2016, our two-person team has grown drastically with the needs of our callers. We started with the aim of providing digital security support to victims of online harassment, however, we soon branched out into providing psychological counseling through a full-time counselor and legal assistance through our legal officer to respond to the dynamic needs of our callers.

Why Online Harassment?

Online harassment and threats that originate from digital spaces are often trivialized and sidelined within mainstream discourse. It has been DRF's mission to mainstream discourse around online harassment and the importance of online spaces.

Online harassment is still trivialized as a form of violence - confined to the virtual world and seen as something you can opt out of.

With the proliferation of the internet and digital technologies, there has been a gap regarding the experience of women who were being targeted in online spaces, and the institutional attention being accorded to it. Extensive research has shown that online harassment can have serious and long-term repercussions on mental health. DRF's research has demonstrated that online harassment can take a psychological toll that manifests itself in depression, chronic stress, generalized anxiety, mistrust, withdrawal as well as insecurity.[1]

[1] Jannat Fazal, "Online harassment: a retrospective review of records", 2017, **https://f1000research.com/slides/6-785.**

In the Pakistani context, there have been unfortunate cases where harassment and blackmailing have resulted in suicide. [2]

Additionally, physical violence looms large over the experience of women and gender non-conforming individuals in Pakistan, and online spaces are no exceptions.[3] Honor killings, social sanctions and threats of violence enabled through digital devices are a daily reality of women in these spaces. Our research reveals that **34%** of women who were surveyed in our Hamara Internet project had experienced online harassment and abuse. Harassment is slowly being normalized as an everyday experience for women online. Furthermore, large percentages of women had witnessed other women being bullied and harassed by men online, of which **55%** agreed that they had. These experiences translated in almost **70%** stating that they were afraid of posting pictures online out of fear that it might be misused. [4]

It has been observed that awareness regarding digital spaces is quite low, both in terms of digital security practices as well as the law that governs them. According to our research, only **28%** of women in our sessions were aware of the *Prevention of Electronic Crimes Act*. Lack of awareness is one of the primary reasons for under-reporting of online harassment.

[2] Mohammad Hussain Khan, "Sindh University student Naila Rind 'committed suicide after exploitation, blackmail': police", Dawn, December 4, 2017, https://www.dawn.com/news/1374502.
[3] Imtiaz Ali, "Engaged couple murdered for 'honour' over accusation of taking pictures together", Dawn, December 3, 2018, https://www.dawn.com/news/1449194/engaged-couple-murdered-for-honour-over-accusation-of-taking-pictures-together.
[4] Sanayah Malik, "Measuring Pakistani Women's Experience of Online Violence", 2017, http://digitalrightsfoundation.pk/wp-content/uploads/2017/05/Hamara-Internet-Online-Harassment-Report.pdf.

Figure 1 Taken from DRF's study "Measuring Pakistani Women's Experience of Online Violence", 2017.

Furthermore, lack of awareness regarding digital spaces is a nation-wide issue.

Figure 2 Taken from DRF's study "Measuring Pakistani Women's Experience of Online Violence", 2017.

Furthermore, individual users in online spaces are disempowered vis-a-viz powerful social media companies whose policies are not transparent and do not provide adequate protection to women according their specific needs.

There is a lack of understanding in terms of knowledge of the local context and the specific needs of Pakistani women. According to our research, only 25% feel that they completely understand the terms and conditions of social media websites.

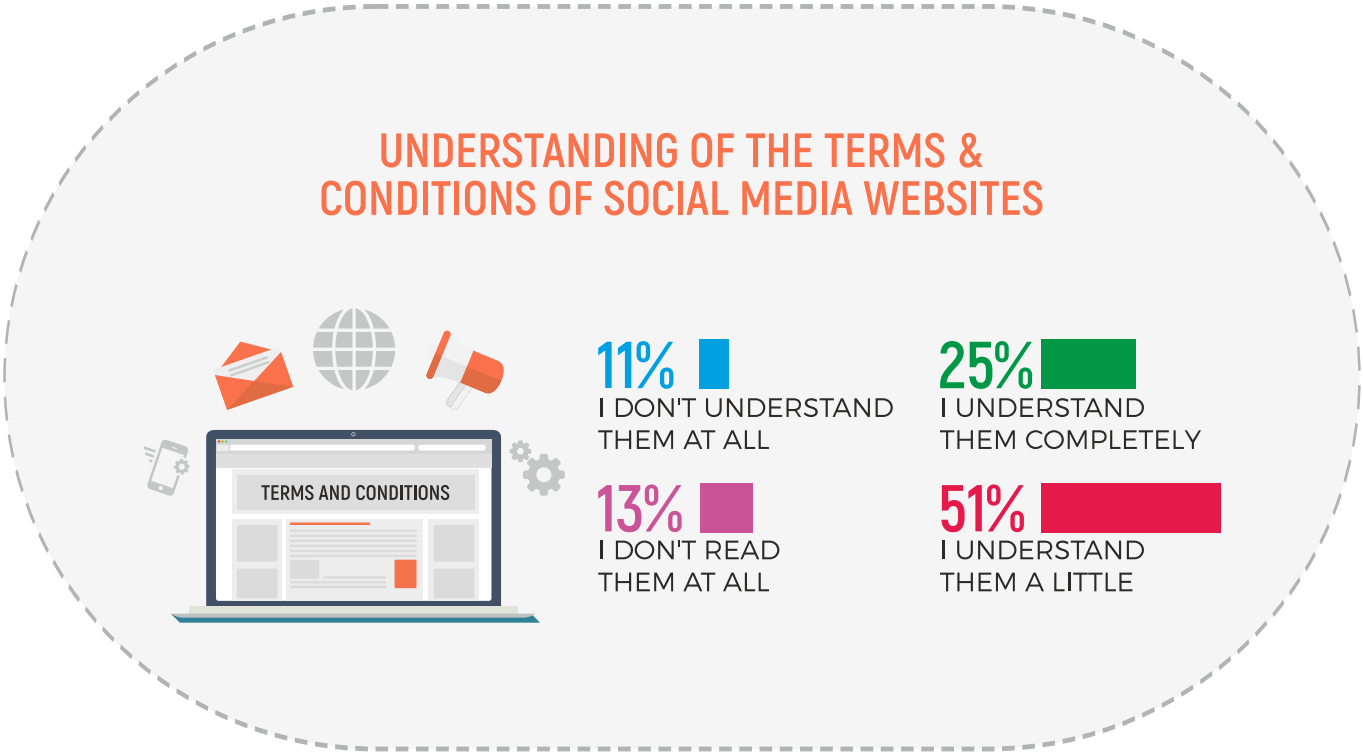

Figure 3 Taken from DRF's study "Measuring Pakistani Women's Experience of Online Violence", 2017.

The cyber harassment helpline aims to fill these gaps in awareness and service delivery. The disparity between the power of individual users and social media companies or government institutions needs to be bridged in order to address online harassment at a systemic level.

Introduction: The Cyber Harassment Helpline

The Helpline seeks to address these gaps in the system by providing a gender-sensitive, confidential and safe space for those facing online harassment. The Helpline Support Staff has developed comprehensive policies around privacy, caller confidentiality and high-quality service.

DRF's Cyber Harassment Helpline is the region's first dedicated helpline for cases of online harassment and violence. The Support Team includes a qualified psychologist, digital security expert, and a lawyer, all of whom provide specialised assistance when needed. The Helpline strives to help women, children, human rights defenders, minority communities and anyone who is made to feel unsafe in digital spaces. Furthermore, we have developed a network of pro bono lawyers and practitioners who can be contacted in case a complainant cannot afford a lawyer. The network draws members from across Pakistan and can be accessed on our website Ab Aur Nahin: https://abaurnahin.pk/.

The Helpline officially began taking calls on December 1, 2016. The Helpline is operational everyday between 9 a.m. to 5 p.m through our toll-free number. The Helpline team can also be contacted outside of office timings through email at helpdesk@digitalrightsfoundation.pk.

This document is part of a series of bi-annual reports by the Cyber Harassment Helpline to ensure transparency of its operations, share its experiences and add to the dearth of data around online harassment in Pakistan. The report seeks to document the data collected by the helpline and provide analysis on trends regarding online harassment as well as policy recommendations to make online spaces safer for all.

Understanding Cyber Harassment in Pakistan through Numbers:

The main medium through which the DRF Support team receives complaints is its helpline number (0800-39393). However, our services are also available on other platforms such as Facebook [5] and email as well. We try to promptly assist complainants and inquirers on any given means of communication, however the helpline is the primary and preferred mode of communication.

The following is an analysis of the number of cases we have received through calls and emails respectively over the last two years.

Total Number of Calls:

From the time the helpline started its journey, we have received a total of **2781** calls from December 2016 to November 2018.

Total Calls
2781

Total New Calls
2190

Total Follow Up Calls
591

In the two years of Cyber Harassment Helpline's operation, the team has provided assistance and support on 2781 calls from all over Pakistan. Out of the 2781 calls, 2190 were first-time callers whereas 591 calls were classified as follow-ups, made by people who were either seeking additional assistance or were providing updates regarding the status of their cases.

[5] Cavet: While we entertain cases on Facebook, if the complainant wants to reveal confidential or sensitive information switch to a more secure mode of communication.

"We reassure our callers to keep in touch with us. This gives them a sense of security and builds a trusting relationship between the caller and the Support Officer"

-Anonymous Helpline Support Staff

The following analysis is based on the two main mediums provided by DRF's Cyber Harassment Helpline: Calls and email.

Keeping in mind DRF's larger principles and mission, the Helpline only collects non-personally identifiable information; thus phone numbers, names and other uniquely identifiable information are not collected. The process of data collection is guided by the Helpline's Privacy Policy that is publicly available on DRF's website and can be provided upon request. [6] The information is also digitally secured, and precautions are taken to ensure data security.

However, in events where someone is in a life-threatening situation or if it has been assessed that during a sensitive conversation that the call might drop, we ask the caller for their consent to temporarily store their phone number so we can get back in touch with them if required. The numbers are not collected in permanent records.

Average Number of Calls:

In the last two years, the Helpline has maintained a monthly average of 91 calls. As can be observed from the monthly breakdown provided below, the number of calls per month has steadily increased, culminating in the last month of November which saw a total of **203** calls.

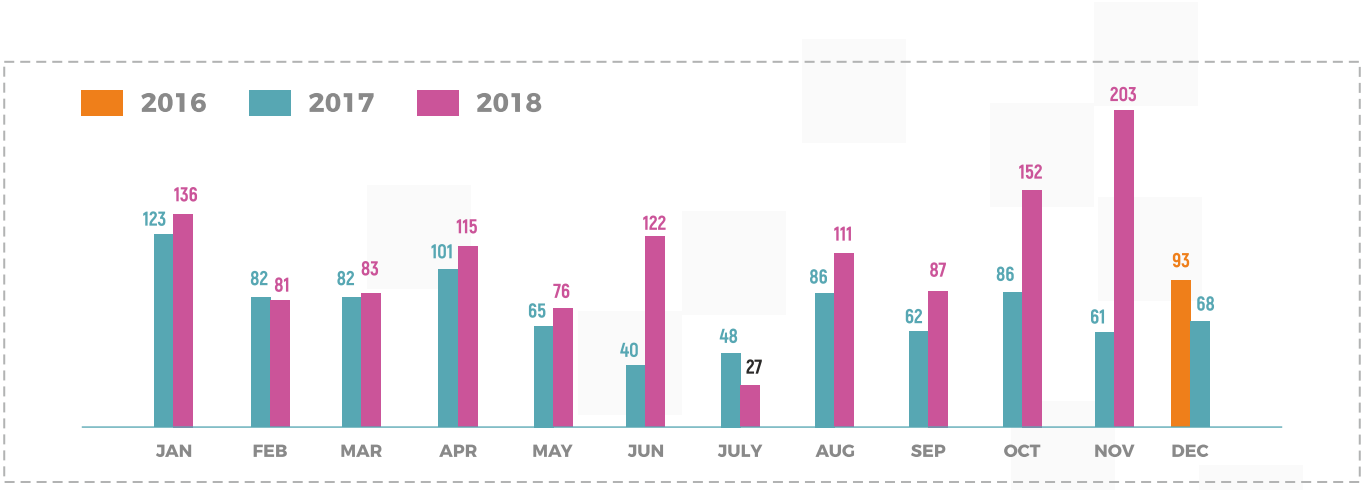

Figure 4 This data is based on the total number of calls attended (2781), not number of individual cases.

[6] "Cyber Harassment Helpline Policy", Digital Rights Foundation, http://digitalrightsfoundation.pk/wp-content/uploads/2017/02/Public-Policy-for-Helpline_30.11.2016-1.pdf.

Average Number of Calls Each Month

91

Total Number of Emails:

In total, **134** people reached out for help through our email platform from December 2016 to November 2018.

Total Emails	Total New Emails	Total Follow Up Emails
134	112	22

Out of the total number of emails, 112 were people who emailed us for the first time and 22 people emailed for follow up concerns or updates. At times, conversations from Facebook or calls were moved to emails so a smoother track of communication could be aligned.

Gender Ratio

Online harassment is a gendered phenomenon as it often experienced by individuals on the basis of their gender.

Our gender-segregated information consists of two sets of data:
1) gender ratio of the callers and **2)** a gender breakdown as per "caller type" that determines whether the caller was calling on someone's behalf or not.

As a standard practice, we do not assume the gender of someone unless they mention it themselves or if it is explicitly confirmed. Creating a safe space for our callers is a process, and we hope to do more in creating a truly gender inclusive and welcoming space. The category of transgender persons and gender non-binary individuals was added in the second year of the Helpline's operations.

Based on our analysis and collected data, 59% of the Helpline's cases were reported by women, 41% were men, and 0.3% were non-binary individuals. It is extremely important to note that these figures are only a depiction of the cases received at DRF's Cyber Harassment Helpline and not a reflection of the overall cases of online harassment in Pakistan or those reported to concerned legal authorities in Pakistan.

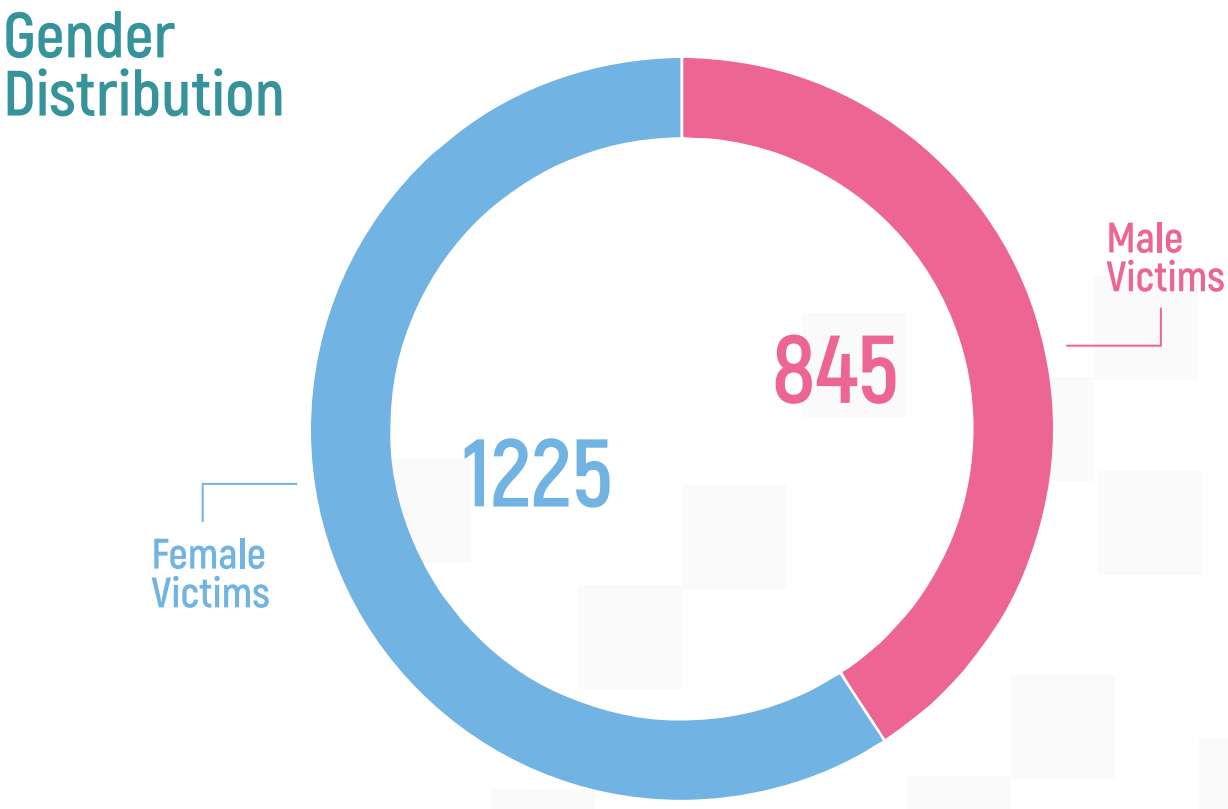

Figure 5 This data is derived from the total number of individual cases (2302), not the total number of calls. The number of female complainants were 1225 and male callers were 845. A small discrepancy of 232 cases exists due the inability to confirm information given the sensitive nature of certain calls.

We have noted that the number of transgender people reporting cases to us are small(13). There are tremendous barriers to reporting cases for transgender individuals and these numbers do not necessarily correspond to the volume of harassment the community faces in online spaces.

Gender breakdown

We also provide below "Gender breakdown" data. This is important in situations where there is a need to understand the disparity between the gender of the caller and the gender of the victim. 86% of our total callers have been categorized as "self," i.e., calling about their own case.

According to our analysis, it is credible that 85% of female callers were calling to complain about their own case, whereas 73% of male callers did so about their own cases. Three transgender reached out to us regarding their own cases as well.

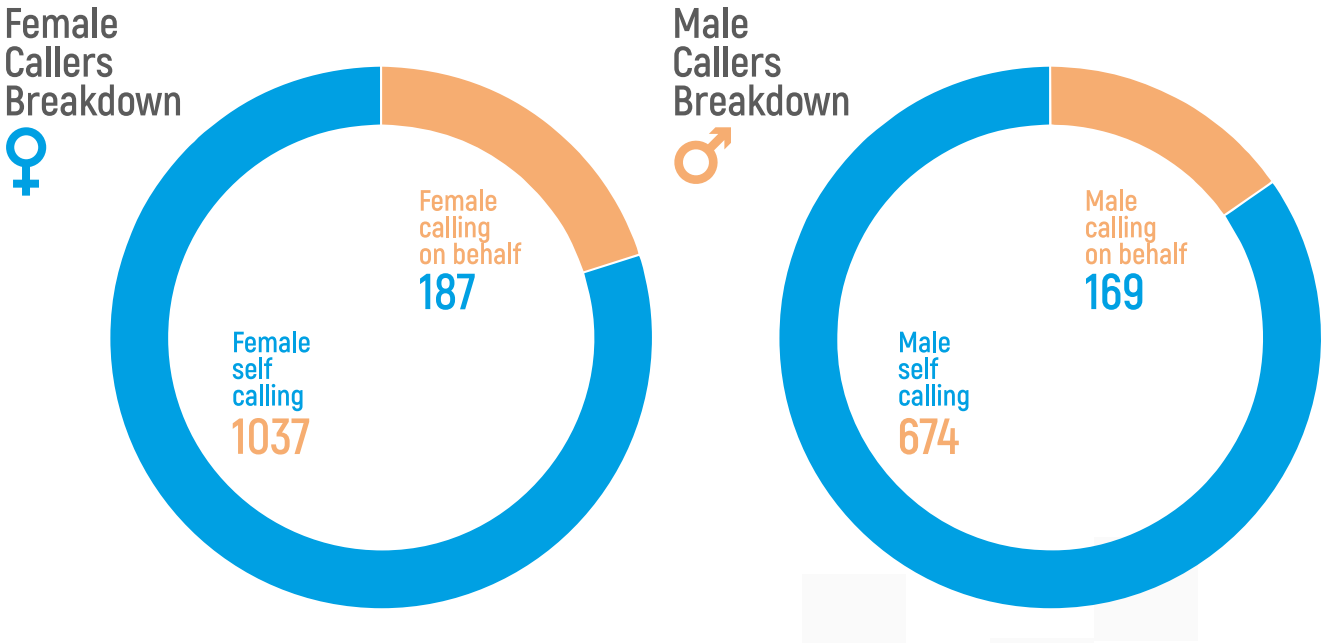

Figure 6 This data is based on the total number of individual cases (2302), not the total number of calls.

Our general observation is that some complainants are hesitant to call for themselves. This is due to a number of factors including the sensitive nature of their cases, inaccess to means of communication or privacy fears. In certain cases, given the trauma experienced by the complainant firsthand, they prefer that someone else speak on their behalf. In cases like these, either a close friend or family member leads the call. Encouragingly, over the past few quarters, the proportion of complainants calling for themselves has risen. We have observed that this reluctance to report their own experiences becomes a challenge to legal remedy since the requires statements from the victim and in person reporting in cases of cyber crime.

Types of Cases

To analyze the general trends of online harassment in Pakistan in greater detail, we categorize the cases according to predetermined typologies that can be found in the appendix.

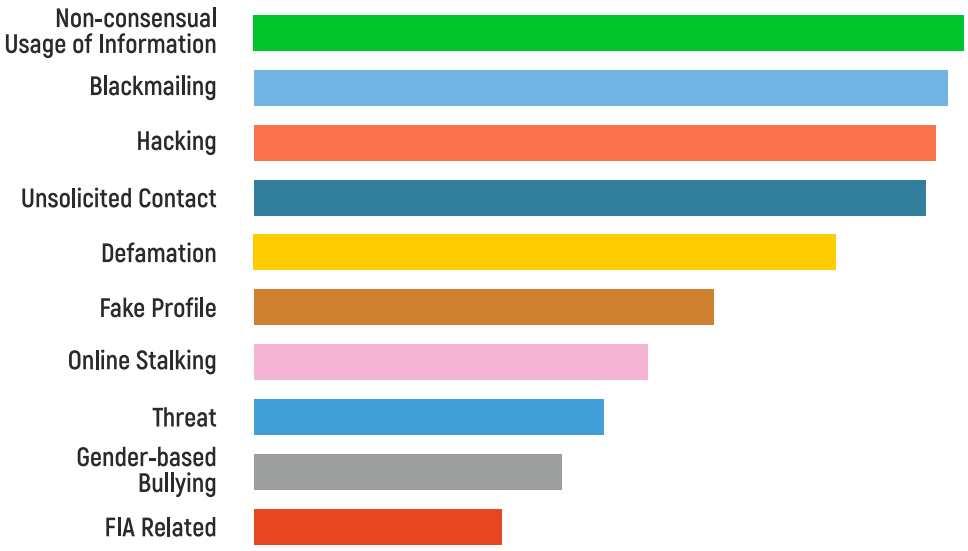

Figure 7 This data is based on the total number of cases. Keep in mind that some callers reported more than one type of complaint. The Helpline Support Staff categorized the nature of the complaint as "secondary" and "primary" according to the facts of each individual case--this data shows the top ten types of cases reported to the Helpline.

It is clear that a majority of the cases are related to non-consensual usage of information (NCUI). These cases involve using, sharing, disseminating, and manipulating data such as photographs, phone numbers, contact details, and other personal information on social media platforms or other websites such as classifieds or networking sites without consent of the individual which violates right to privacy.

The second most common calls involved blackmailing, which often entail using an individual's personal information or psychological manipulation to make threats and demands. Other most commonly reported cases include hacking and unsolicited contact.

Notably, in the past two months, the Helpline has experienced an influx of calls relating to mobile-based scams that prey on the trust of individuals. One of the most common types involve deception to gain WhatsApp codes of mobile users, which in turn leads to the hacking of their WhatsApp account. The scammers claim to be from legitimate organizations, ranging from television game shows, Pakistan Army, government departments such as the Benazir Welfare Programme and telecommunication companies.

Geographical Distribution

To understand the geographical patterns of harassment cases across the country and the outreach of the Helpline itself, information regarding the city or area of residence is collected.

Keeping in line with the policies regarding data privacy of Helpline, the callers are neither required to provide their address nor does the Helpline Staff keep it in records.

A majority of the cases received by the Helpline were from **Punjab (57%)**, the most populous province in Pakistan. The second highest number of cases were received from **Sindh (15%)**.

Provincial Distribution

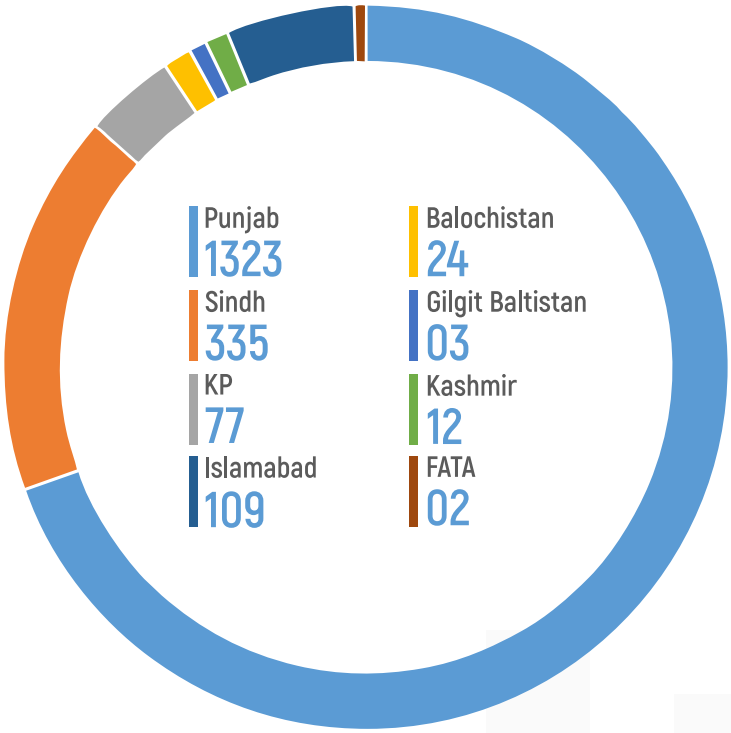

Figure 8 This distribution is based on the number of individual cases. The significant number of missing data is in cases where either it was deemed inappropriate to ask for location data, or when the complainant refused to provide it.

(In) accessibility to FIA's Offices

Access to Law Enforcement Agencies (LEAs) is one of the most important determinants of the smooth functioning criminal justice system. Previously, FIA's National Response Centres for Cyber Crime (NR3C) offices were only located in Islamabad, Rawalpindi, Peshawar, Quetta, Karachi, and Lahore. However, towards the end of 2018, FIA was allowed to open 15 new cybercrime centers all over Pakistan to combat the increase in cybercrime. The FIA's procedure for reporting requires the complainant to travel to the NR3C's office in person and register their case to commence legal proceedings. 37% of the cases the Helpline receives come under the domain of the FIA.

A majority of the cases received at the Helpline were from urban districts, with Lahore, Karachi and Islamabad in the top three. It is also interesting to note that a vast majority of the calls were from cities where offices of the NR3C, FIA where located, which meant that the remaining 19% came from places without an office creating geographical impediments to reporting. This is a vast improvement from last year, and it is important to acknowledge that the percentage of complainants living in cities without an office has gone down since the expansion of NR3C offices.

City Distribution

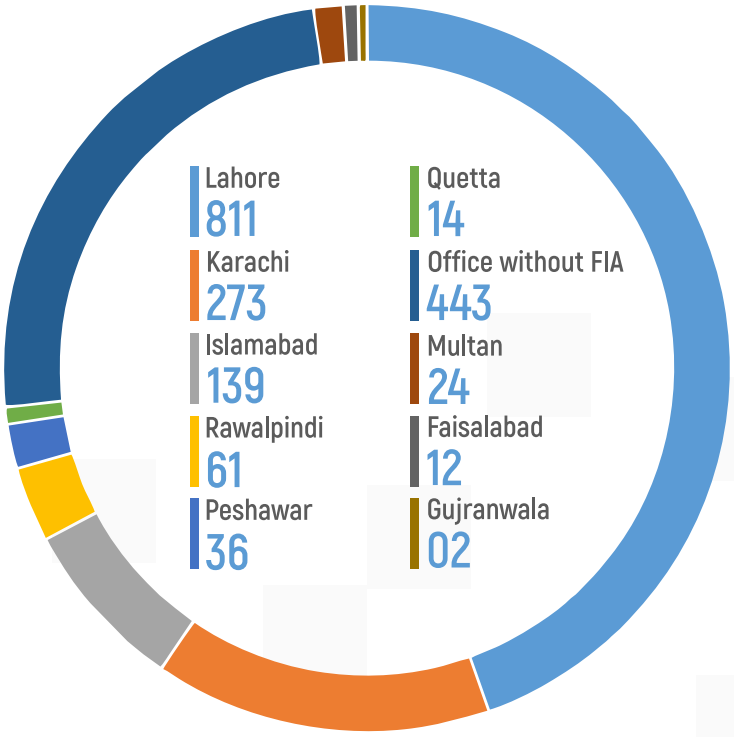

Figure 9 This data is based on the number of individual cases.

Age Distribution

A majority of our callers (21%), were between the ages of 21 to 25 years. Read with the gender ratio discussed earlier, it can be deduced that the most vulnerable demographic regarding online harassment contacting the helpline are young women.

It is also interesting to note that 2% of the complainants were under the age of 18, which is below the age of majority and consent. Callers under the age of 18 present challenges in terms of reporting since many of them are not receiving support from their legal guardians. Furthermore, cases become even more complicated in instances where the alleged harasser is also younger than 18.

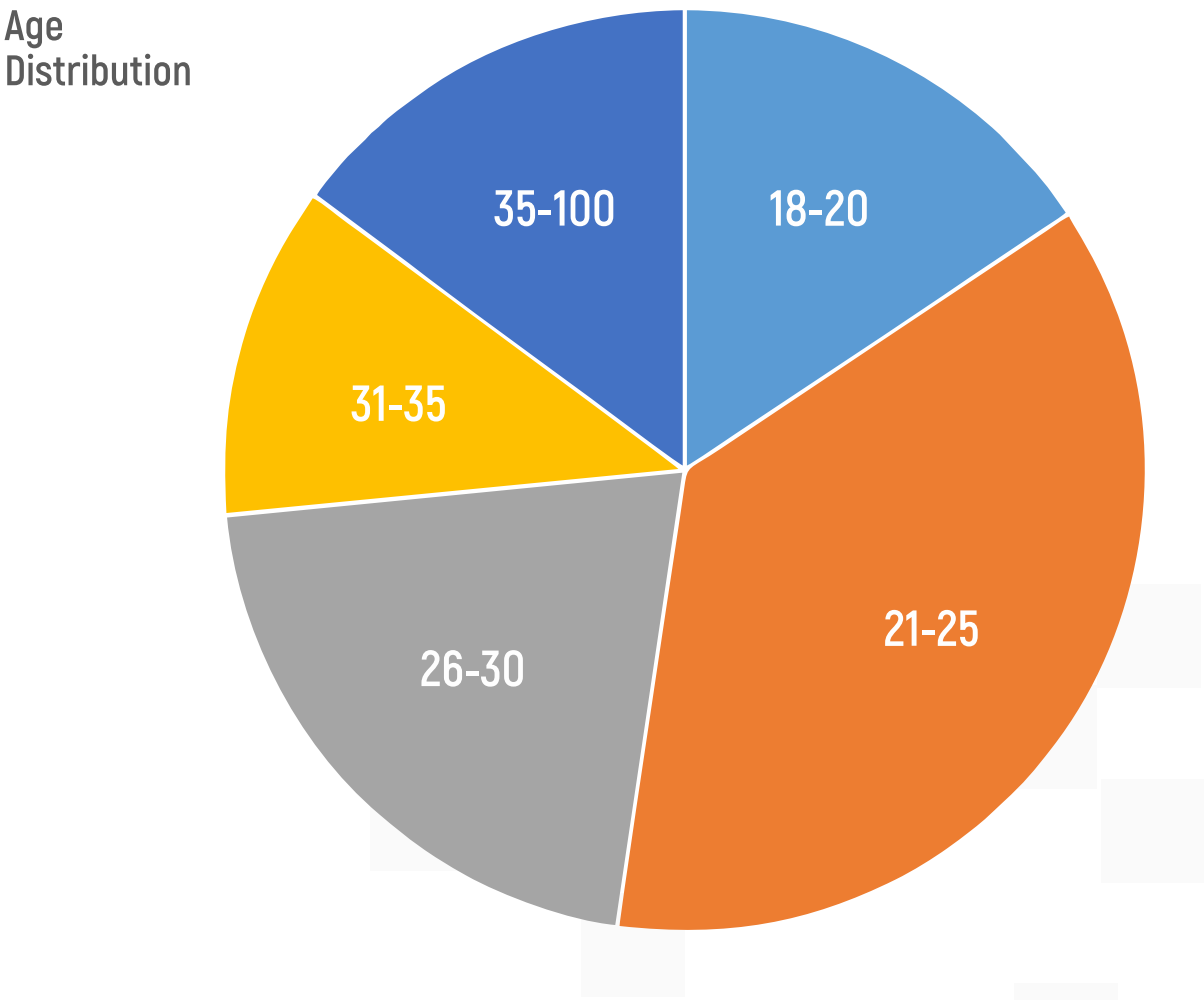

Figure 10 This data is based on individual cases, not the total number of calls.

Platforms

The internet is increasingly becoming a complicated and multi-layered space with several dominant social media companies, as well as smaller platforms. As a result, the Helpline deals with cases of harassment on multiple digital platforms. Through Figure 11 (below) we identify the mediums and social media platforms that are the most common sites for harassment. This distinction is important because it highlights not only the spaces most prone to harassment but also which policies, sets of community guidelines and laws apply in certain cases.

The companies that own these platforms are diverse in their policies, community guidelines and mechanisms to address harassment. Furthermore, since most of these companies have offices in foreign jurisdictions, there is often a cultural, language and legal barrier when it comes to reporting cases of online harassment. By far the biggest number of complaints at the Helpline relate to Facebook (**660** complaints)—**29%** of our callers experience harassment on Facebook.

Recently, there has been an influx of cases regarding **WhatsApp** which is reflected in the fact that cases regarding the messaging application have risen from 2.6% to 9.5% in the past six months (with the total number of cases rising from 29 to 220).

Figure 11 This data is based on individual cases, not the total number of calls.

Referrals

Given that DRF is a non-governmental organization, there are limitations to our investigative and intervention powers. When a caller wants to pursue a legal case or investigate into the identity of their harasser, the Helpline Staff informs them about the National Response Centre for Cyber Crime (NR3C) of the Federal Investigation Agency (FIA) as the designated law enforcement agency (LEA) as per section 29 of the Prevention of Electronic Crimes Act 2016 (PECA). Nevertheless, the final decision is with the caller whether they want to follow through with the referral. As is evident in the figure below, 37% of our cases are either fully or partially referred to the FIA, given that it is the designated agency under PECA for legally filing cases. For cases within Lahore, our legal officer accompanies complainant to the FIA offices and actively follows up on cases in the Lahore branch. For other cities, we have established contacts in various branches in order to refer cases effectively.

In sensitive situations or emergencies that require immediate action from Law Enforcement Agencies or when specialized services are needed, our Staff refers the case to other relevant government authorities or NGOs for further assistance such as the PCSW, Rozan and LoBono in Karachi.

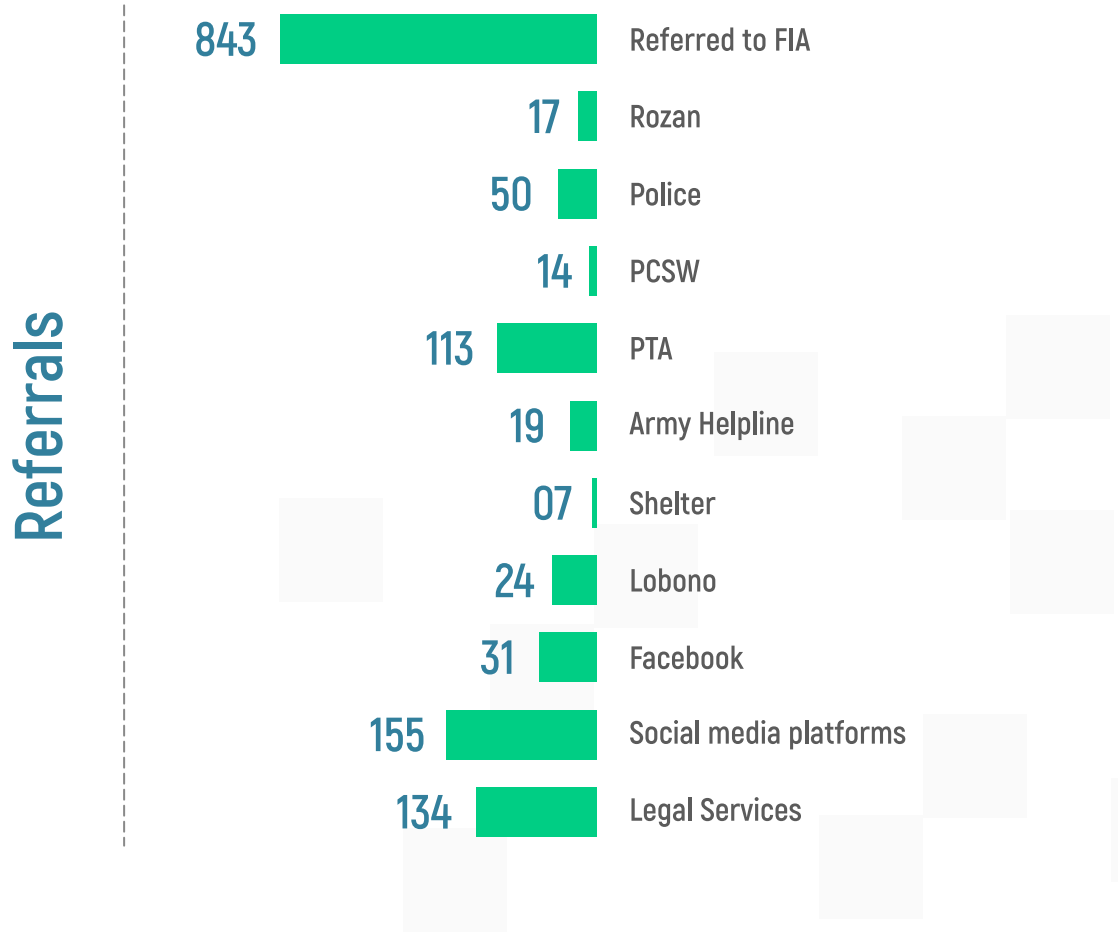

Figure 12 This data is based on the total number of individual cases, not number of total calls attended.

Where do People Hear About our Helpline?

To understand the impact of our communication efforts, we ask our callers about where they first heard about us. A majority of our callers have heard about us from social media or through word of mouth. The Helpline team, along with our advocacy officer, regularly run awareness campaigns online to educate users about digital safety and for outreach regarding out helpline.

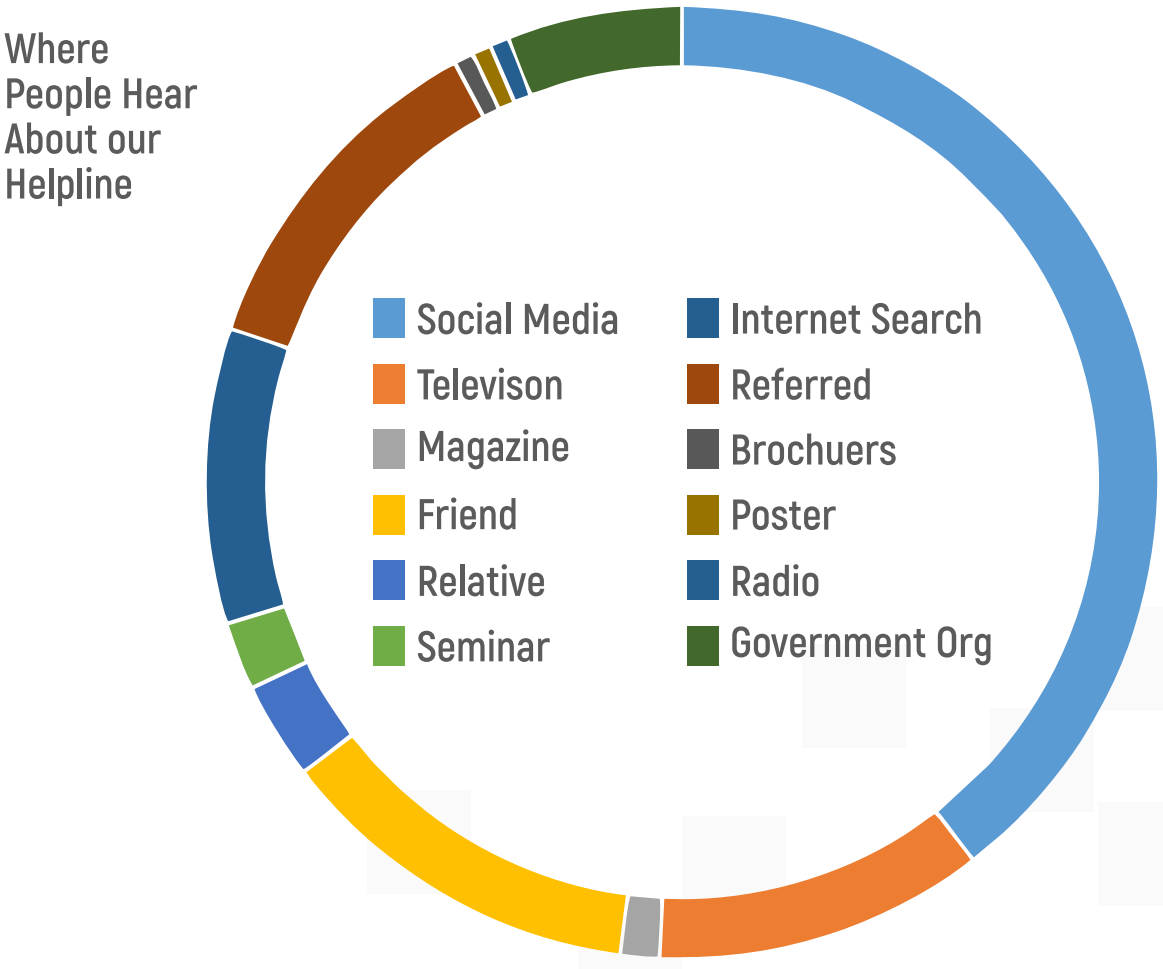

Figure 13 This data is based on individual cases, not the total number of calls.

Types of Services Provided

Cyber Harassment Helpline provides either one or a combination of services:

1. **Legal Counsel:** We inform people about their rights and the options they have under the cyber law.
2. **Digital Security Support:** We provide relevant digital support required to secure the individual in an online space.
3. **Mental Health Counselling:** We lend a non-judgemental ear to distressed individuals to help them cope with their situations.

The following is a breakdown of the services provided on cases:

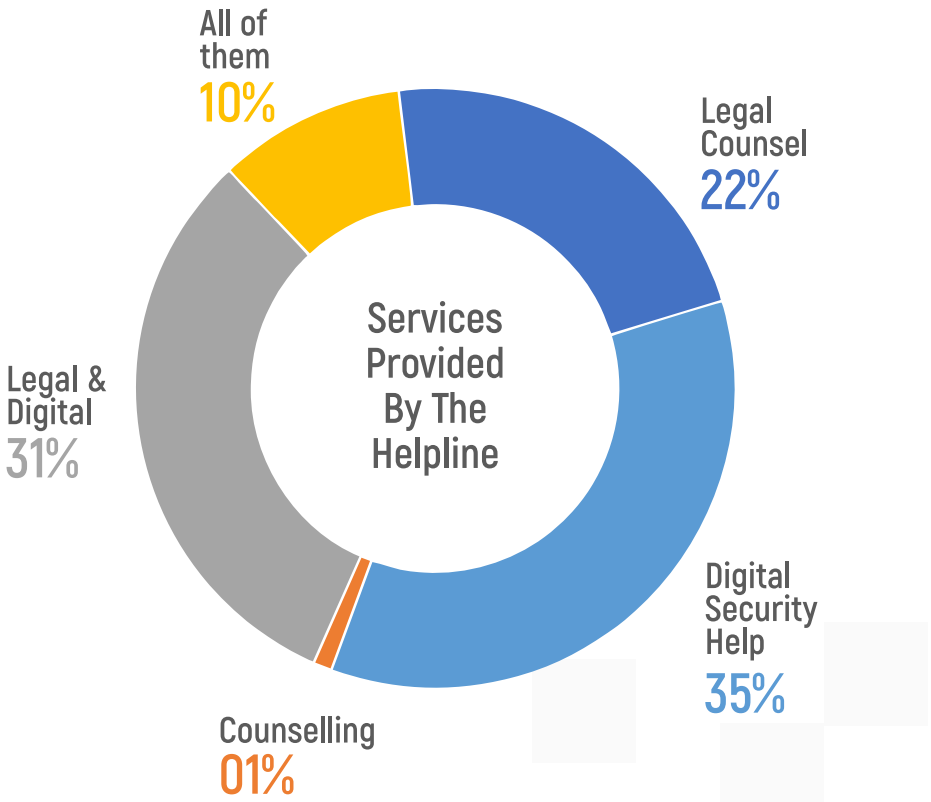

Figure 14 This data is based on individual cases, not the total number of calls.

A majority of our cases deal with complainants requiring digital security assistance, which is provided by the Helpline staff trained in basic digital security and well versed with the community guidelines of social media companies to facilitate reporting.
In cases requiring legal counsel or assistance, our dedicated legal officer provides telephonic and in-person services as well. “Ab Aur Nahin” acts as a network of pro bono lawyers who can step in when complainants are looking for quality and affordable counsel.

Callers at Risk

Individuals with Mental Health Issues:

Our Helpline team assesses every distressed caller against mental health indicators and looks out for signs in individuals for minimal or extreme suicide ideation. Suicidal ideation means thinking about or planning suicide. Thoughts can range from a detailed plan to a fleeting consideration. An interesting analysis made in the two years of the helpline's operation is that **26 males** and **18 females** were noted to have suicidal ideations.

Our helpline support staff are specifically trained to offer psychological support to the callers; however, in any case where an individual is deemed to have extreme suicidal ideation, he/she is immediately referred to our in-house Psychologist.

According to our observation, men don't come out with their psychological issues within their family or peers due to internalized roles of masculinity that contradict the concept of asking for help or support when dealing with emotions. Thus, men are more likely to reach out for help outside their support circles.

Individuals from Vulnerable Communities:

We received calls from complainants who were deemed to experience heightened vulnerability online due to the fact that they belonged to marginalized communities and groups. **07** such cases were received from individuals who identified as gender and sexual minorities. Some of these callers were specifically targeted by individuals for personal reasons, while others were victims of harassment online and offline simply because of prejudice against their gender and sexuality. It has been observed that these individuals are common targets of such hate crimes.

2 calls have been received from callers who identified themselves as belonging to religious minority groups and an additional **2** identified as ethnic minorities. **1** caller who reached out to us was physically disabled. Receiving calls from communities that are stigmatized or marginalized, even though not many, highlights that these issues are not only endemic to women but speaks to targeting of groups deemed as vulnerable or different in these spaces. Members of marginalized communities are less likely to reach out and have less access to resources for assistance, which means that the statistics here are not representative of extent of threats faced by the community.

Case Studies

Exploitation of Minors through Sexually Explicit Images:

A hacker used the details of a 17-year-old girl's Snapchat ID to gain access to sexually explicit personal pictures saved in the memories section of the application. This resulted in extensive blackmailing on part of the hacker, threatening to release her pictures if she refused to send him more pictures.

Owing to the fact that this involved blackmailing and sexual images of a minor, DRF referred the case to the Punjab Commission on the Status of Women (PCSW) so that it could be dealt with in a gender-sensitive manner. Our legal officer set an appointment to accompany the complainant to the PCSW office so that her application could be submitted.

The Vulnerability of Women in Media

A member of the Pakistani entertainment industry approached us when sexually explicit videos and pictures consensually shared with her ex-partner were leaked on the internet. Her videos and pictures were distributed on different pornographic websites and social media platforms. The Helpline team escalated complaints that involved private sexually explicit content.

Consequently, dozens of links containing sexually explicit content were taken down within a matter of days as DRF was able to leverage its partnerships with various platforms to escalate the complaints and send take-downs requests in a timely manner.

Harassment by a family member

An unidentified individual was contacting a complainant and her friends through a fake profile with extremely abusive and threatening messages. The complainant wished to find out identity of the harasser, thus the Helpline team provided legal counsel and set up an appointment for her with a law enforcement officer so she could file her case immediately. After a thorough investigation and follow-ups from the Helpline staff, it was revealed that the harasser was her fiance. This revelation caused a lot of psychological distress to the complainant and she as soon as she expressed suicidal ideation, our counsellor made sure that she was regularly seeing a therapist. The Helpline team also routinely checked up on her to ensure that she did not feel isolated. The complainant chose not to pursue the case in court, however she severed all ties with her fiance.

Detailed accounts of these stories are available in our report, ***"Experience of Online Harassment in Pakistan: Case studies from the cyber Harassment Helpline".*** [7]

[7] "Experience of Online Harassment in Pakistan: Case studies from the cyber Harassment Helpline", Digital Rights Foundation, December 2018, https://digitalrightsfoundation.pk/work/research/.

Emerging challenges

Online spaces are extremely dynamic and the trends emerging within Pakistan are evolving with the techno-legal landscape. We've compiled a list of emerging challenges that we have observed through the cases we receive:

- **Whatsapp Hacking:**
  Hacking of social media applications, especially WhatsApp accounts is an emerging and worrying trend. Hackers scam people by obtaining their WhatsApp codes, in turn, gaining access to their WhatsApp accounts and group chats. These scams are usually perpetrated by impersonating government officials, telecom companies or schemes like Benazir income support or Jeeto Pakistan. By the time a victim realizes that their account has been hacked it's usually too late and they are already banned from the application or defamatory messages have already been disseminated. It's important to address the gravity and expanse of this problem as in just the month of November Helpline has received around 90 cases concerning WhatsApp hacks. We urge users to be mindful of the information they share with strangers and also understand that passwords and codes are personal data and should not be shared with anyone.

- **New FIA Cyber Crime Wings:**
  Gender sensitization and capacity building of the officials at the newly setup cybercrime wings of FIA, in different cities of Pakistan, have become a concern for us. It's very difficult for victims to come forward with their complaints because of victim blaming and it becomes an uphill battle when the Investigation Officers do not create a welcoming environment for the complainants.

Future Roadmap

Helpline's team since its inception has been working diligently to provide the best of services to the victims of cyber harassment. Their struggle and hard work will reflect in advocating and strengthening through the following ways in the upcoming years:

Outreach

The helpline has not used any commercial means to spread awareness of the services provided to victims of cyber harassment or to raise awareness regarding cyber harassment. The problem is widespread and serious, and to address that, the helpline will increase its outreach not just in urban areas but in rural areas as well. All across Pakistan through radio advertisements and awareness sessions.

Jurisprudence

Interpretation of law is needed for resolution of disputes and justice, but since cybercrimes act (Prevention of Electronic Crimes Act, 2016) is relatively new, jurisprudence has not been developed on it. Our legal officer at the Cyber harassment helpline will follow up on cases to ensure there prosecution and ultimately developing jurisprudence for easier application and interpretation of existing laws.

Sustainability of Helpline

We would like to acknowledge our donors for their support and trust in our work; this would not have been possible without them. We hope that people will understand the significance of our work and continue to support us.

Recommendations

We recommend that the government and FIA expand its resources for tackling online harassment by increasing the number of offices for the NR3C. DRF also appreciates the inclusion of civil society groups in the planning stage; giving civil society voice at the table ensures diverse representation and better decision-making. Nevertheless, there is a long way to go in terms of addressing online harassment, and we hope that the incumbent government continues to see online harassment as a serious and pressing issue.

1 **PECA Rules:** It has come to light that the Rules u/s 51 of PECA have been drafted by the Ministry of Information Technology, more than two years after the passage of the law. These Rules have not been made public, and the government is under an obligation to ensure that the forthcoming PECA Rules are compatible with principles of human rights—particularly the right to freedom of expression, the right to privacy and protection of minorities. The Rules should expand the rights available to citizens and guarantee protections against intrusion in their digital spaces rather than further curtailing them.

2 **Greater resource allocation:** While there has been a vast improvement in the resources allocated to the NR3C than in the past, we posit that more needs to be done to keep up with the exponential growth in cybercrime cases at the NR3C. The Interior Ministry has approved for 15 new reporting centers to be built across the country, some of which are already operational. According to the FIA's figures, not only have the number of cases increased, but the rate of growth of complaints has also grown (complaints rose 20% from 2015 to 2016, while there was a 30% rise from 2016 to 2017). Since the NR3C's Phase 3 proposes to cover the five years, it means that the increase in resources should neither be limited to meet the current demand, nor the current rate of growth. The FIA recently stipulated in a Senate hearing that it only has 10 cybercrime experts at its disposal. With the increased access to ICTs and awareness regarding cyber crimes, the FIA will need to respond to an unprecedented number of complaints. The allocation of resources, thus, needs to take into account these unique circumstances and DRF urges the concerned government departments to increase grants allocated to the FIA.

3 **Mechanism to deal with cases in foreign jurisdictions:** In many cases where either the accused or the complainant is located outside Pakistan, the NR3C lacks the capacity to take action despite being empowered to do so u/s. 1(4) of PECA. This is further exacerbated by the fact that that there is no Mutual Legal Assistance Treaty (MLAT) between Pakistan and any country where offices of social media companies are located. Pakistan is not a signatory to the Budapest Convention on Cybercrime, which sets up a regime for international cooperation on cybercrime. DRF recommends that there be at least one officer in each branch dealing with cases in foreign jurisdictions, with specialized training in international law and conflict of laws. Both the Ministry of Information Technology and Interior Ministry are urged to define "international cooperation" u/s 42 of PECA while upholding the spirit of the rights of Pakistani citizens.

[8] Qadeer Tanoli, "Ministry allowed to fill 415 vacant posts," The Express Tribune, September 10, 2018, https://tribune.com.pk/story/1799249/1-ministry-allowed-fill-415-vacant-posts/.
[9] Munawer Azeem, "FIA allowed to open 15 centres to check cybercrime", Dawn, October 3, 2018, https://www.dawn.com/news/1436438.
[10] "FIA has only 10 cyber crime experts, Senate body told", Pakistan Today, Jun 22, 2018, https://www.pakistantoday.com.pk/2018/06/22/fia-has-only-10-cyber-crime-experts-senate-body-told/.

4 **Regular reporting and performance review of the FIA:** DRF urges the FIA to fulfill its obligations u/s 53 and submits bi-annual reports, something it has failed to do in two successive six-month periods. Furthermore, based on the reports there needs to be an assessment of the FIA's performance predicated on the feedback from complainants and litigants and performance markers such as the rate of conversion from a complaint to an FIR, number of women whose cases were registered and performance reviews of investigators and prosecutors. These reports should also be made available online.

5 **Sex-disaggregated data:** The FIA, while fulfilling its statutory obligation to report to Parliament u/s 53 of PECA, is requested to produce data regarding the number of online harassment cases and the number of cases registered by women under each section of PECA, particularly sections 21 and 24. These figures should be public and will allow for better policy-making and allocation of resources.

6 **Creation of a separate desk for online harassment within the NR3C:** Given the specialized nature of online harassment cases and the gender-sensitivity required for complainants/victims, DRF recommends that a dedicated desk for cyber harassment be set up within the NR3C to handle cases u/s 21 and 24 of PECA. This desk should be the point of first contact for complainants of online harassment and equipped with officers specifically trained in the nuances of online harassment, its various forms, and gender-sensitivity as well as counseling services

7 **Rapid Response Cell:** Given the urgent nature of certain cases of online harassment, where leaked information can harm personal safety or cause immediate reputational harm, a rapid response cell that is operational 24/7 should be established in addition to the regular operations of the NR3C. Cases marked as urgent should be expedited and dealt with on a priority basis.

8 **Privacy and Confidentiality:** One of the biggest barriers for reporting cases of cybercrime, particularly online harassment, to law enforcement is the fear of leaked information and a further breach of confidentiality. Many complainants require the assurance of confidentiality as a prerequisite to reporting. The FIA is thus urged to develop clear, accessible and publicly available Standard Operating Procedures (SOPs) on privacy, confidentiality, and protection of evidentiary data and identity of the complaints. These SOPs should be compliant with best practices regarding data protection, translated into regional languages and displayed clearly in all offices of the NR3C. At a larger level, there is a dire need for a data protection legislation that safeguards the data of citizens held by private government bodies. The Ministry of Information Technology is urged to expedite the legislative process around a personal data protection law.

9 **Greater accessibility for disabled persons:** Functioning elevators, ramp for wheelchairs, accessible toilet facilities and in-person assistance in filing applications are minimum requirements that every NR3C office should meet to ensure that disabled persons do not have to face additional hurdles in registering and pursuing complaints.

10 **Coordination with other departments:** Given the intersecting nature of online and offline spaces, cases often involve both online and offline crimes, complainants are often given contradictory advice regarding the jurisdiction of the police and NR3C. In certain trials given that challans contain both sections of PECA and PPC, there is often back and forth between different courts and judges. DRF recommends that channels of communication between police stations and cybercrime stations be established to ensure that cases can be easily transferred and there is clarity as to where a particular case be registered, investigated and prosecuted.

11 **Empower local police to process cases of online harassment:** While cases under PECA are under the jurisdiction of the FIA, the role of the police and its infrastructure can and should be harnessed to ensure that cybercrime is processed at the local level.

12 **Psychological services:** DRF urges the FIA to make provision for psychological services at NR3C offices to help complainants deal with the psychological trauma and distress that they experience due to online harassment and violence. All officers at the NR3C, especially those dealing directly with victims, should be given training on how to address trauma. The NR3C should offer a safe space for victims and help them process with their trauma in a constructive and safe manner.

13 **Case management and tracking system:** Complainants should be able to track and receive regular updates on the status of their case through an accessible and easy-to-use case management system/portal. Digital copies of the case file and evidence filed should be stored on a secure server to ensure reliable duplicates in case the original case file is lost or tampered with.

14 **Gender sensitization:** Several female complainants who have approached the NR3C have reported being shamed for their choices and discouraged from pursuing cases by officers at the NR3C. DRF has observed that while higher officials, such as Deputy Directors and Assistant Directors, are sensitive to these issues and proactively reassure complainants, this attitude is not always reflected in the behavior of individual IOs. Since many cases involve sharing of intimate data and gendered harassment, there is a need to ensure that the officers (especially those directly dealing with complainants), as well as the overall environment of the offices, are conducive to female complainants and provide a safe and judgment-free space. DRF recommends that a quota of at least 33% female Investigation Officers and Prosecutors be instituted, and all officers—including the female ones—be given extensive gender-sensitivity training. It is also recommended that women's rights organizations be included and allowed to assist in developing these trainings. Furthermore, gender sensitization does not only mean taking into account the specific needs of women but different genders such as non-binary and transgender. Often gender nonconforming individuals are the most vulnerable to harassment and are subsequently discouraged from reporting the same.

15 **Check on the performance of investigators and prosecutors:** Internal mechanisms should be in place to review the performance of investigators and prosecutors. The incompetence and insensitive behavior of these officers towards the complainant can lead to a miscarriage of justice in certain cases. Complainants should be able to register concerns and complaints regarding their assigned officers to a senior presiding officer to each regional zone, which should automatically trigger an independent and transparent inquiry.

A new officer should be assigned immediately in case of misconduct or failure to perform duties.

16 **Greater technical expertise:** Several complaints to the NR3C experience a substantial investigative delay or are dropped completely due to lack of technical abilities of officers and technologies available to the FIA. DRF recommends that measures be taken to capacitate them to not only meet current trends in cybercrime but also keep abreast with developments in the five-year coverage period. This capacity building should be an on-going and constant process. Thus, DRF recommends substantial investment in research at the NR3C to address the needs to litigants/complainants.

17 **Training for judges on cybercrime law, internet governance, and online harassment:** Internet governance and cybercrime should be included in the curriculum of provincial judicial academies to ensure that judges are not only familiar with the law regarding the internet, but also have a thorough understanding of the technologies involved in the process. It has been observed that judges are not only ignorant of the law regarding the internet and cybercrime, but that they also fundamentally misunderstand the governance and infrastructure of the internet itself, which leads to bad jurisprudence and, at times, "unimplementable" orders.

18 **Collaboration with civil society organizations:** DRF recommends more public-private partnerships by the government to ensure that the public institutions work collaboratively with civil society and academia to complement each other's work. A mutually beneficial MOU between DRF's cyber harassment helpline and NR3C will be in the best interest of victims and will ensure the complainants obtain timely and comprehensive support.

Appendix:

Types of Cases:

In order to analyze the needs of the Helpline as well as general trends of online harassment in Pakistan in greater detail, we categorize the cases according to predetermined typologies. The following are definitions that we use to sort the cases:

General Inquiry: These are inquiries we receive regarding cyber harassment, digital security, and the work of Digital Rights Foundation. This category also includes inquiries that we get outside the realm of digital rights, in which case our Helpline Support Staff redirects the caller to the relevant authorities and organizations through the referral network.

Impersonation: Complaints under this category involve an individual's identity being appropriated without their permission. This manifests itself in profiles purporting to belong to someone on social media websites and contacting people through texts or calls pretending to be someone else.

Blackmailing: This often involves using personal information or psychological manipulation to make threats and demands from the victim. Blackmailing using sexually explicit videos or pictures is criminalized under section 21 of the Prevention of Electronic Crimes Act 2016 (PECA).

Stolen Device: These complaints involve loss of information, data, and identity in cases where digital devices are stolen or misplaced. Assistance provided involves helping complainants in recovering and securing their accounts as well as assisting them in filing criminal complaints about theft.

Fake Profile: Fake profile on a social media platform or application is an account pretending to be someone or something that doesn't exist.

Scam Calls: Fraudulent calls that pretend to be an individual or from an authority to make a quick profit. Mostly such scam calls lead to a potential financial fraud being committed.

Abusive Language: Using harsh, hurtful, explicit or insulting language to attack another person.

Unsolicited Contact: Unsolicited contact involves unwanted and repeated calls and messages by the accused/abuser, which may include spam, repeated requests for contact, personalized threats, blackmail or any unwanted contact that makes the receiver feel uncomfortable. If this rises to the level of criminal liability, cases in this category can fall under the ambit of section 24 of PECA.

Login-Issues: These involve difficulties in accessing accounts and devices where the user has been locked out or has limited/compromised access due to a known or unknown reason.

Hacking: Gaining unauthorized access to someone's electronic system, data, account, and devices which can result in loss of data, loss of identity and blackmailing.

Federal Investigation Authority (FIA)-related Inquiry: These are queries we get regarding the complaint procedure of the National Response Centre for Cyber Crime (NR3C) of the FIA. These callers often want to file a formal, legal complaint. It also includes individuals who are contacting the Helpline after they have dealt with the FIA, either to get advice on their case or to complain about the FIA officials or process.

Non-Consensual Usage of Information (NCUI): This involves using, sharing, disseminating and manipulating data such as photographs, phone numbers, contacts, and other personal information without consent and in violation of the privacy of a person.

Online Stalking: Online stalking is keeping track of someone's online activity in a way that it makes the subject of the stalking uncomfortable. For the purpose of this report, online stalking also refers to (repeatedly) contacting a person's friends and/or family.

Doxxing: Doxxing is the practice of leaking and publishing information of an individual that includes personally identifiable information. This information is meant to target, locate and contact an individual, usually through social media, discussion boards, chat rooms and the like; and more often than not, is accompanied by cyberbullying and cyberstalking.

Gender-based Bullying: Any actions, statements, and implications that targets a person based on their gender identity or sexual orientation. Evaluations for gender-based bullying take into account the overall connotations attached to actions and verbal communications within the larger system of gendered oppression and patterns of behavior that signify abuse.

Bullying: Any actions, statements, and implications that targets a person in order to intimidate, silence, threaten, coerce or harass them. This category is distinguished from the one above, where the complainant is targeted specifically on the basis of their gender.

Non-Consensual Use of Pornographic Information (NCUPI): This is obtaining, using, distributing or retaining pictures, videos or graphic representations without a person's consent that violate their personal dignity.

Financial Fraud: Intentional actions of deception perpetrated by a person for the purpose of financial gain and profit; this includes using someone's financial data to gain access to accounts and make purchases. For the purpose of our operations, we confine our definition to fraud conducted through electronic means.

Stalking: This category includes monitoring, physical following, and harassment that occurs outside of online spaces. A majority of the cases received by the Helpline relate to non-consensual use of information, which include pictures, videos, and personal data. In cases of online harassment, this information is weaponized by harassers to cause harm, reputational damage or to blackmail victims. This information is also manifested in fake profiles or used on various forums without the consent of the victim.

Another major form of harassment experienced by our callers is unsolicited messages, usually containing lewd or threatening content.

Non-Consensual Photoshopped Pictures/Doctored Pictures: The manipulation, distortion or doctoring of images without the permission of the person to whom they belong. This is often accompanied by distribution and sharing, or threat to share, of such pictures as well.

Threats of Sexual/Physical Violence: An action or verbal communication that results in a reasonable fear of sexual or physical attack.

Non-Cooperation from Social Media Platforms: These complaints refer to a situation when a person has reported a case of cyber harassment to the relevant social media team but has not received a decision in their favor.

Threats: These are all threats directed at the victim of online harassment that do not fall under the category of gender-based threats or sexual/physical violence.

Defamation: Any intentional, false communication purporting to be a fact that harms or causes injury to the reputation of a natural person.

Hate Speech: Any communication that targets or attacks an individual on the basis of their race, religion, ethnic origin, gender, nationality, disability, or sexual orientation. Hate speech becomes a matter of urgent action when it puts its target in physical danger or the reasonable apprehension of physical danger. However hate speech is not restricted to just incitement to violence, it is hate speech if it leads to the exclusion of or creation of a hostile online environment for its target.


DRF
Digital
RightsFoundation
“KNOW YOUR RIGHTS”