CYBER HARASSMENT HELPLINE

ONE YEAR REPORT

DECEMBER '16 - NOVEMBER '17

Digital Rights Foundation

"KNOW YOUR RIGHTS"

ABOUT

Digital Rights Foundation envisions a place where all people, and especially women, are able to 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 a healthy and productive environment that would eventually help not only women, but the world at large.

ACKNOWLEDGMENTS

On the completion of its first year, the Helpline Team would like to thank all the people who supported the project and used their respective platforms to amplify our voices. To anyone who has referred a case to us or shared a post about us, we are deeply indebted to you. Online harassment continues to be trivialised, however with your help we've been able to start a conversation around the subject.

We would not be here without the support of our wonderful donors--Urgent Action Fund, Digital Defenders Program, Open Tech Fund and the Dutch Foreign Ministry (Dutch Human Rights Tulip Award)--who believed in our vision from the very start, sustained our work and helped expand our services.

Most importantly, we would like to thank anyone who picked up the phone and have given us a call. Your stories, feedback and courage have buoyed us and continue to be a source of inspiration.

CONTENTS

BACKGROUND:
ONLINE HARASSMENT

Digital Rights Foundation (DRF) is a pioneering organization in Pakistan working on issues of online harassment, technology and gender through research, advocacy and service delivery. Online harassment and related threats are often trivialized within mainstream discourse, and not accepted as a form of violence. It has been DRF's mission to mainstream conversations around online harassment and the importance of online spaces.

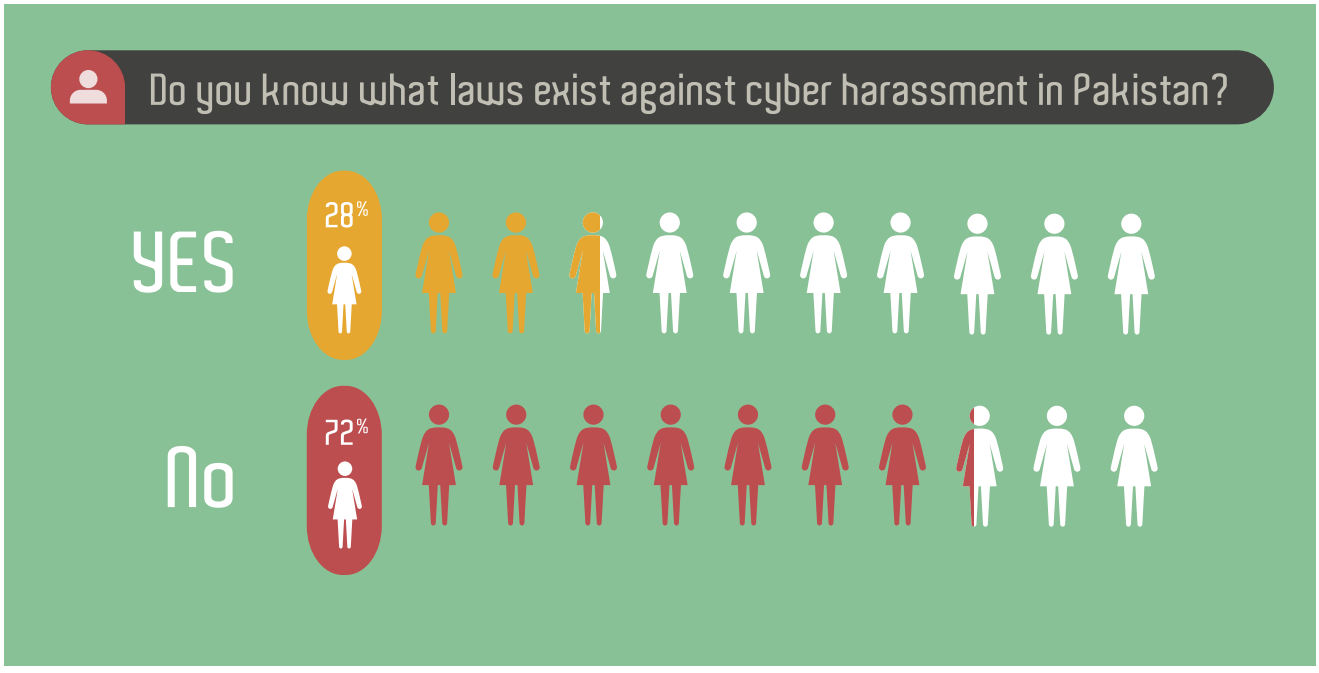

Figure 1: Level of awareness regarding online harassment laws in Pakistan.[1]

The Cyber Harassment Helpline was launched after the successful completion of the Hamara Internet (translates as "Our Internet") project, and based on its findings in the "Measuring Pakistani Women's Experience of Online Violence" report.[2] Our research has sought to dispel myths that digital rights are a fringe concern; the Hamara Internet campaign revealed that 79% of young women used digital technologies on a regular basis, which shows that this is a subject that affects a vast majority of the population.

---

[1] *"Measuring Pakistani Women's Experience of Online Violence", Digital Rights Foundation, May, 2017, http://digitalrightsfoundation.pk/wp-content/uploads/2017/05/Hamara-Internet-Online-Harassment-Report.pdf.*

[2] *Note 1.*

Figure 2: Frequency of technological use among young Pakistani women.[3]

The use of these technologies is gendered and informed by the positionality of particular users. Young women are much more likely to self-censor their activities online and experience online harassment. This makes them more vulnerable in online spaces, along with other groups such as religious minorities and activists in Pakistan.

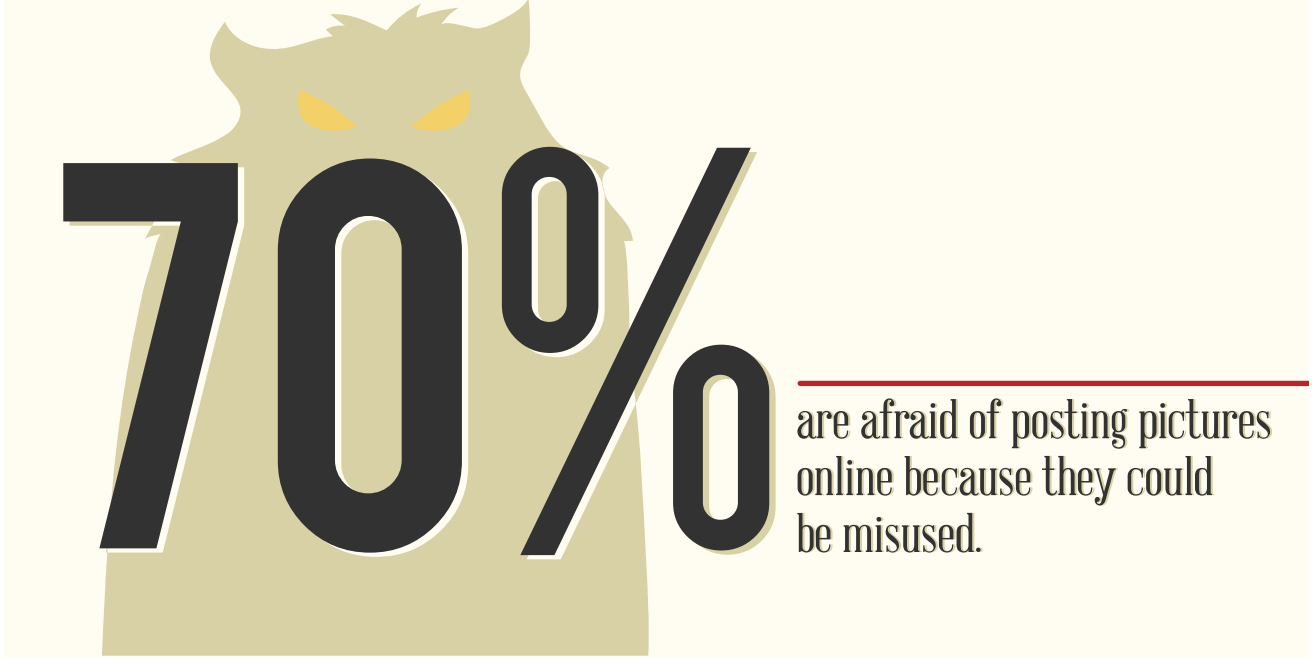

Figure 3: Measuring the proportion of women who hesitate before posting online.[4]

[3] *Note 1.*

[4] *Note 1.*

Figure 4: Measuring the proportion of women harassed online.[5]

DRF has observed a serious gap when addressing online harassment in individual cases. Confidence in existing law enforcement agencies dealing with online harassment is low (Figure 6). This resulted in several women reaching out to DRF regarding their cases of online violence and harassment; and in turn, these cases are the impetus for streamlining our efforts and to institutionalize the capacity to address individual complaints.

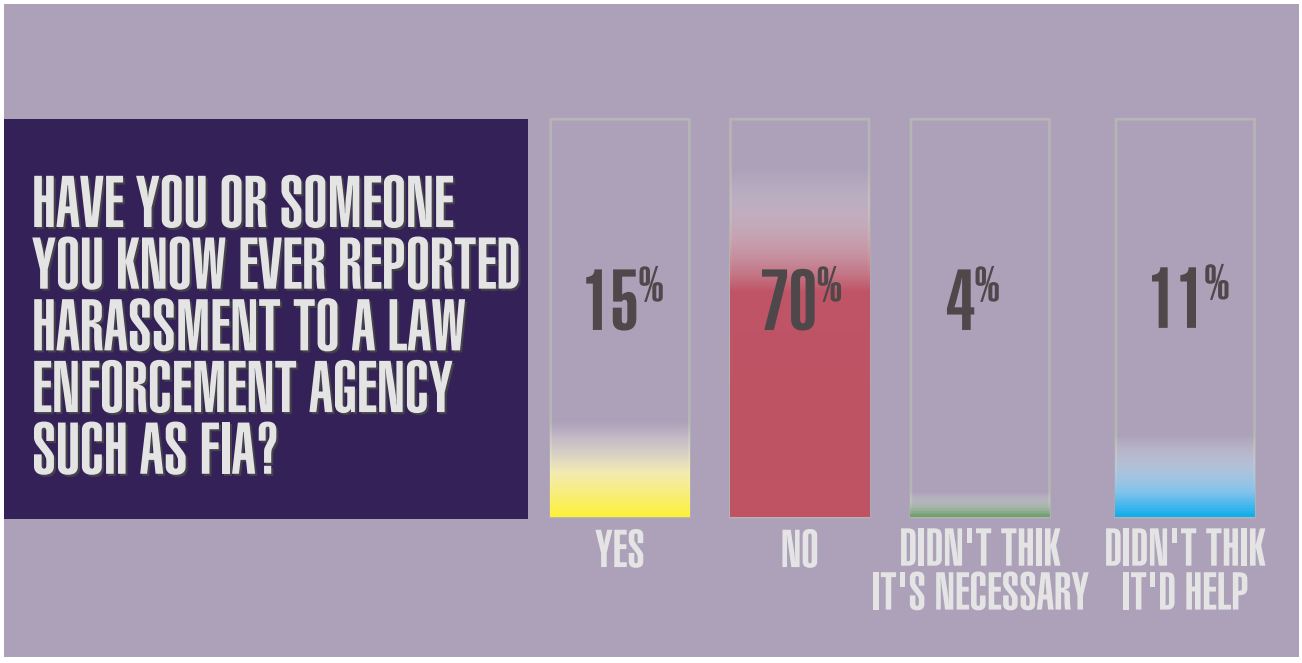

Figure 5: Measuring rate of reporting online harassment among women.[6]

[5] *Note 1.*

[6] *Note 1.*

Figure 6: Reasons women hesitate in reporting online harassment.

The Helpline seeks to address these gaps in the system and problems that women face by providing a gender-sensitive and confidential space for those facing online harassment. The Helpline Support Staff has developed comprehensive policies around privacy, caller confidentiality and quality control to ensure that a safe space is created for its callers.

ABOUT:
PAKISTAN'S FIRST CYBER HARASSMENT HELPLINE

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, legal officer, all of whom provide specialised assistance when needed. The Helpline strives to help women, children, human rights defenders, minority communities—and anyone who feels unsafe in digital spaces.

The Helpline officially began taking calls on December 1, 2016. The Helpline is operational everyday between 9 a.m. to 5 p.m. 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.

Goals and Objectives of the Helpline

The overarching goal of the Helpline is to contribute towards addressing online harassment, taking into account the specific needs of women and marginalized communities within the Pakistani context.

By way of clarification, the Helpline does not seek to replicate the work of law enforcement and investigative agencies; in fact, our aim is to complement those efforts. Thus, the Helpline does not investigate cyber crimes; that is the domain of the state and should remain so, subject to due process and requirements of criminal procedure. Our efforts are directed at making these institutions more accountable and track their progress once cases have been referred to them.

Objectives for the first year

1) Increase awareness of digital safety among complainants;
2) Provide a safe, judgement-free, gender-sensitive and confidential environment for victims to share their experiences of online harassment;
3) Give direct and quality mental health counselling to victims who exhibit signs of psychological distress;
4) Provide digital security solutions;
5) Awareness of digital rights by providing legal advice to complainants regarding online harassment law, procedure of filing a criminal complaint and setting realistic expectations of legal remedy;
6) Provide a comprehensive referral system to complainants who wish to obtain specialized services or to callers whose complaint does not fall within the ambit of online harassment;
7) Collect non-personally identifiable information to be used for purposes of advocacy and research;
8) Produce and publish regular operational and transparency reports that are publicly available.

SUCCESS INDICATORS

- ✓ Satisfaction of Individual Callers
- ✓ Development of robust protocols and policies for the helpline
- ✓ Maintenance of steady number of calls throughout the year
- ✓ Outreach outside urban centers
- ✓ Development of a comprehensive and responsive referral system in partnership with various service delivery, civil society, and government organisations

HELPLINE DATA: UNDERSTANDING CYBER HARASSMENT IN PAKISTAN

Total number of cases:

The primary channel for communication for the Helpline is its toll-free number; however, the Support Staff also handles complaints over email and Facebook inbox as well.[7] The Helpline has received 1,551 complaints in the form of calls, emails and Facebook messages in its first one year, from December 1, 2016 to November 30, 2017.

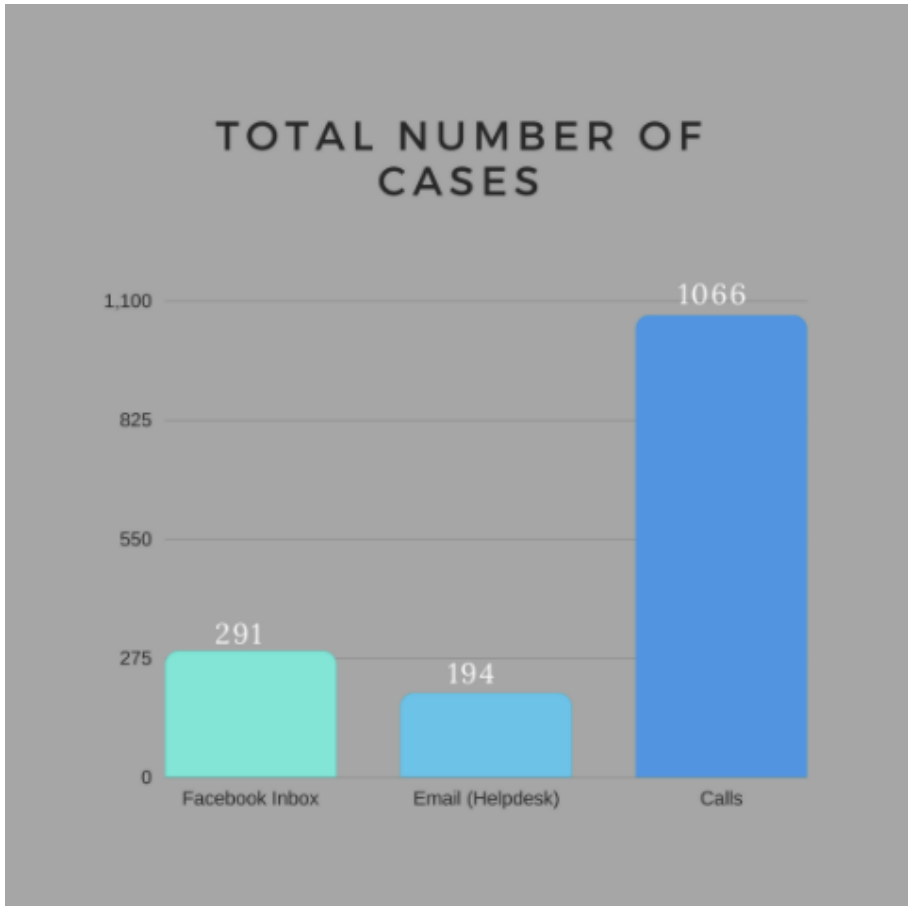

Figure 7: This breakdown is based on the number of individual complaints, and not the total number of calls, messages and emails that we received.

[7] *As per Helpline Policy, while the Helpline does entertain complaints through its Facebook page, it does not encourage or advertise this mode of communication given concerns of confidentiality and Facebook's data sharing policies.*

Volume of Calls:

In its first year, the Cyber Harassment Helpline attended and provided services to 1476 calls on its toll-free number. Out of the total number of 1476 calls, 1066 were first time callers and 410 were follow-up calls from people who were either updating their assigned officer about their case or seeking additional information/assistance.

Total Calls	**1476**
Total New Calls (Individual Cases)	1066
Total Follow-up Calls	410

AVERAGE NUMBER OF CALLS PER MONTH

123

calls each month on the Cyber Harassment Helpline

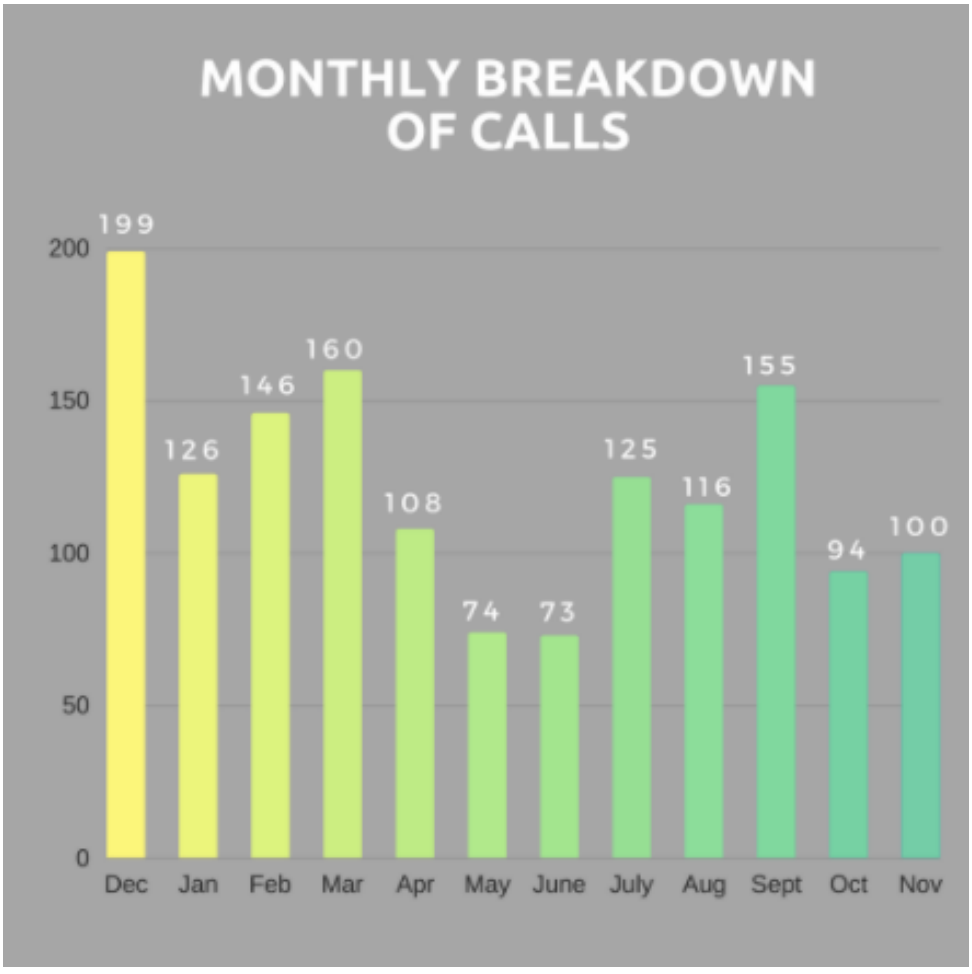

Figure 8: This data is based on the total number of calls attended (1476), not number of individual cases.

The Helpline Support Staff only collects demographic information from the callers, and not through Facebook or email. For this reason, the following analysis is based exclusively on calls, which is the primary service provided by the Helpline.

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 is 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.[8] The information is also digitally secured and precautions are taken to ensure data security.

Gender Ratio:

Online harassment is experienced primarily by women, an observation that is backed up by data. 3,252 out of 12,339 complaints (26.36%) for cyber crime at the National Response Center for Cyber Crime (NR3C) are by female complainants.[9] We conduct our gender analysis using two sets of data: 1) gender ratio of the callers, and 2) a gender breakdown as per "caller type."[10]

---

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

[9] *Source: The National Response Center for Cyber Crime (NR3C), FIA, from 18th August, 2016 to November, 2017*

[10] *We categorize caller-type along these lines: a) "self": the caller is calling about their own case; b) "on behalf of a friend": the caller is not experiencing the harassment first-hand, but calling to report the harassment experienced by a friend; and c) "on behalf of a family member": the caller is not experiencing the harassment first-hand, but calling to report the harassment experienced by a family member.*

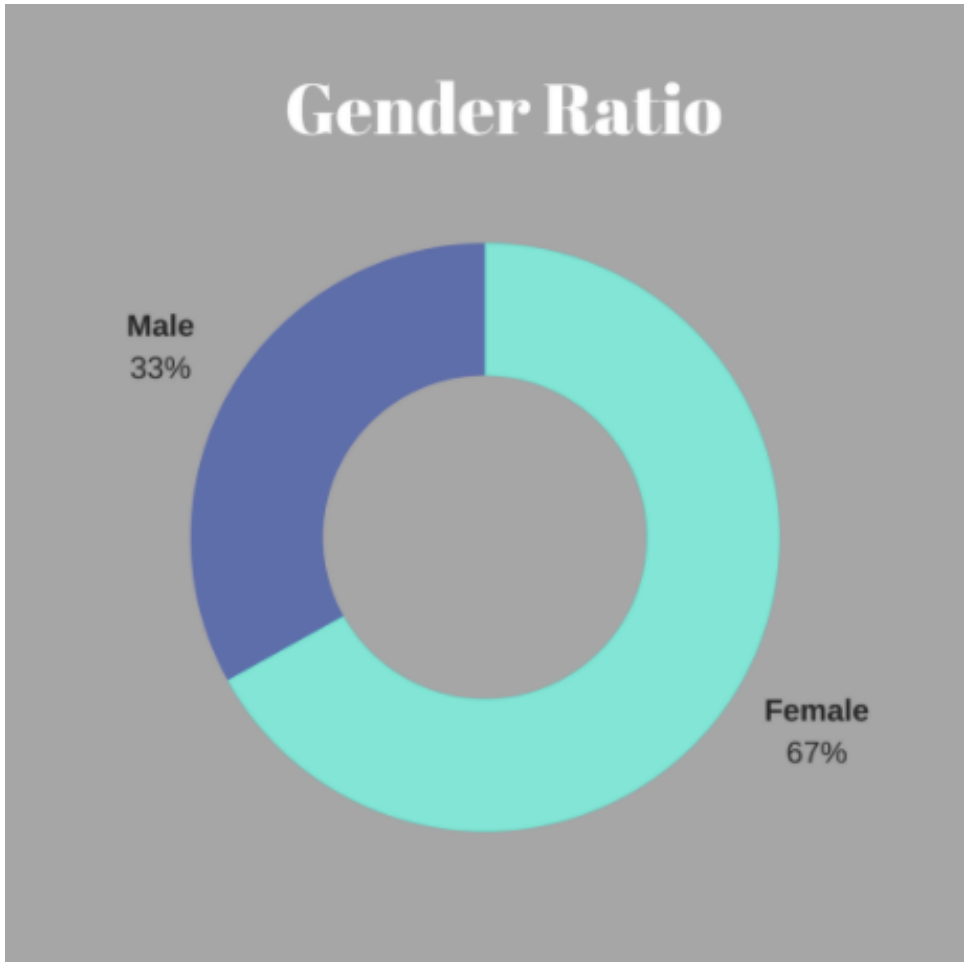

Figure 9: This data is derived from the total number of individual cases, not the total number of calls. The number of female callers were 692 and male callers were 342. A small discrepancy of 32 exists due the inability to get confirm information given the sensitive nature of certain calls.

872 (82%) of our total callers have been categorized as "self", i.e. calling about their own case. Thus, the gender data needs to be contextualised further to account for the callers who are calling on behalf of someone they know. In order to account for these situations we provide the "Gender Breakdown" data.

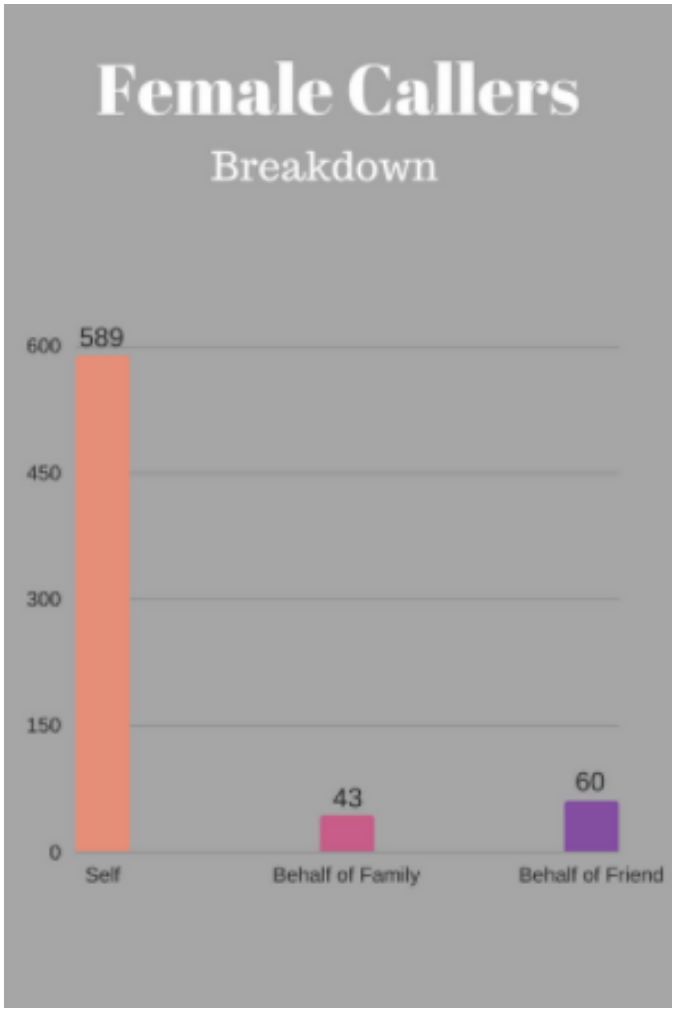

Figure 10: This data is based on the total number of individual cases.

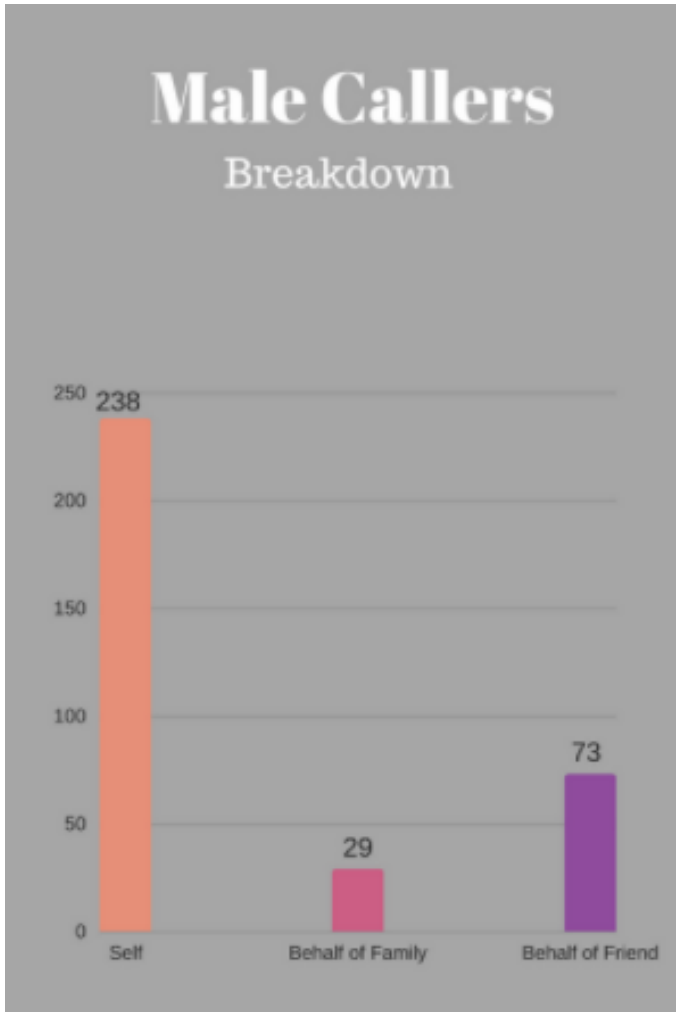

Figure 11: This data is based on the total number of individual cases.

It is apparent from the data that 85% of female callers are calling regarding their own complaint, while only 70% of male callers were calling regarding their own case.

Types of Cases:

In order to better analyse the needs of the Helpline as well as general trends of online harassment in Pakistan, 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 someone's identity being appropriated without their permission. This manifests itself in profiles purporting to belonging 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.

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 for theft.

Unsolicited Messages: Unsolicited messages are unwanted and repeated contact by the accused/abuser, which may include spam, repeated requests for contact, personalised threats, blackmail or any unwanted messages that make the receiver feel uncomfortable.

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

Hacking: Gaining unauthorized access to someone's electronic system, data, account and devices.

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 persons 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 behaviour 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.

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 the 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 favour.

Stolen Device: Cases where personal information, digital safety or privacy is compromised as a result of theft or misplaced electronic device.

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.

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.

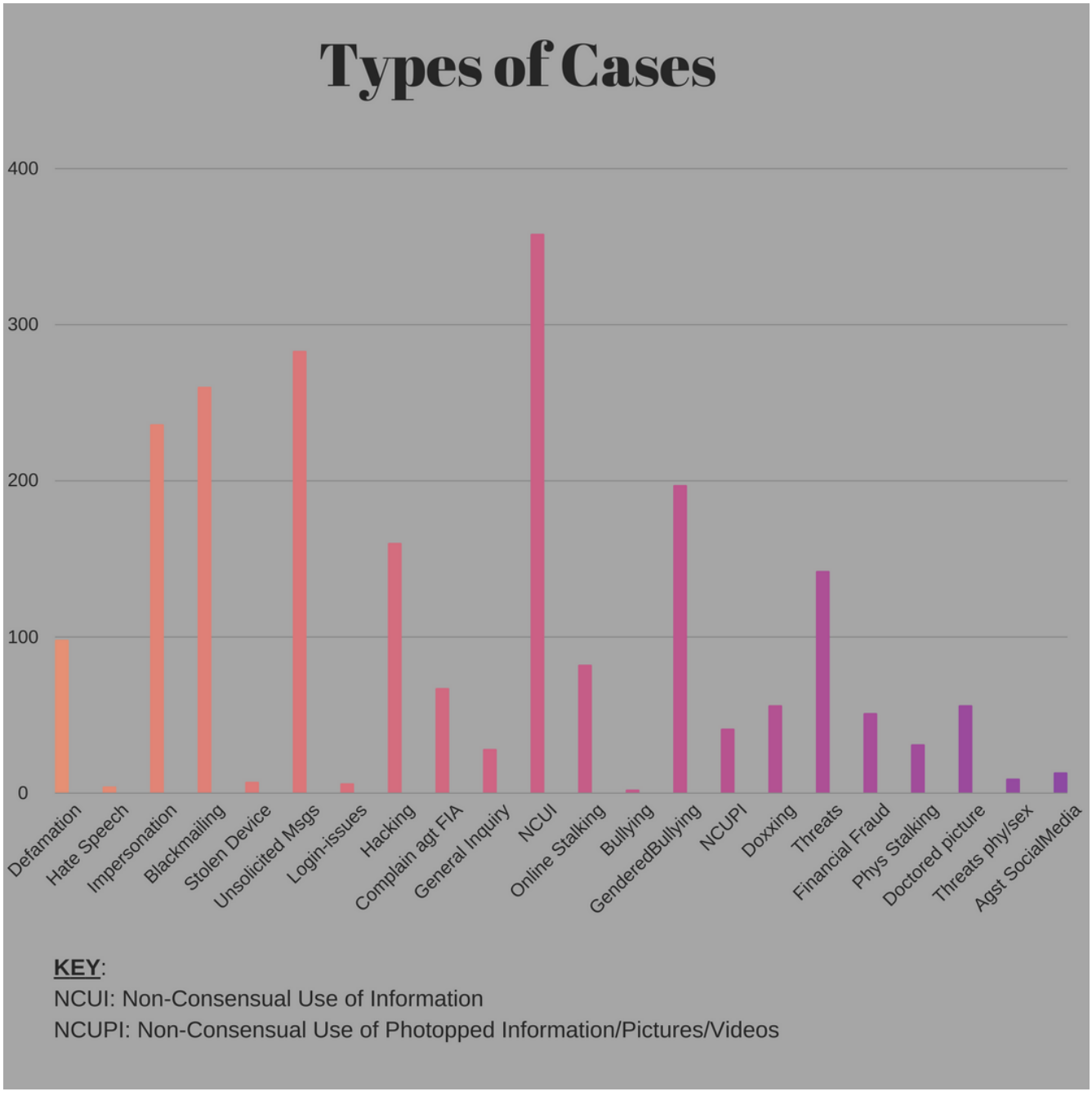

Figure 12: This data is based on the total number of cases. Keep in mind that some callers reported more than one type of complaint. The Helpline Support Staff categorized the nature of the complaint as "secondary" and "primary" according to the facts of each individual case.

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 and spaces. Through Figure 13 (below) we wish to 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 (480 complaints)—45% of our callers experience harassment on Facebook.

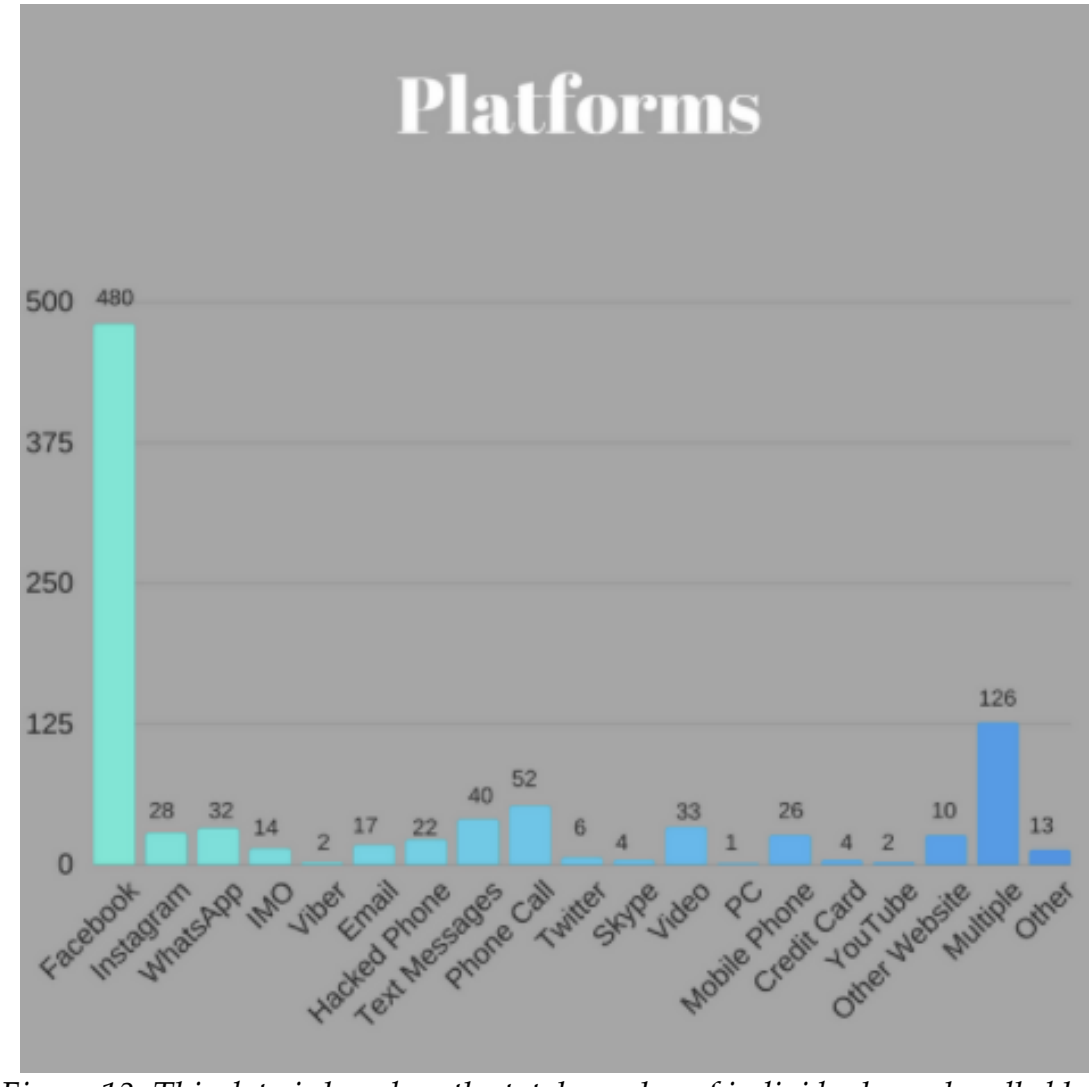

Figure 13: This data is based on the total number of individual case handled by the Helpline. There is a discrepancy of 154 cases as this category of data was not adequately and systematically obtained in the first month of operations (December).

Referrals:

Given that DRF is a non-governmental organization, there are limitations to our investigative powers. When a caller wants to pursue a legal case or investigate 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) tasked with investigation of cyber crimes. Nevertheless, the final decision is with the caller whether they want to follow through with the referral. In emergencies that require immediate action from LEAs or when specialised services are needed, our Staff refers the case to other relevant government authorities or NGOs for assistance.

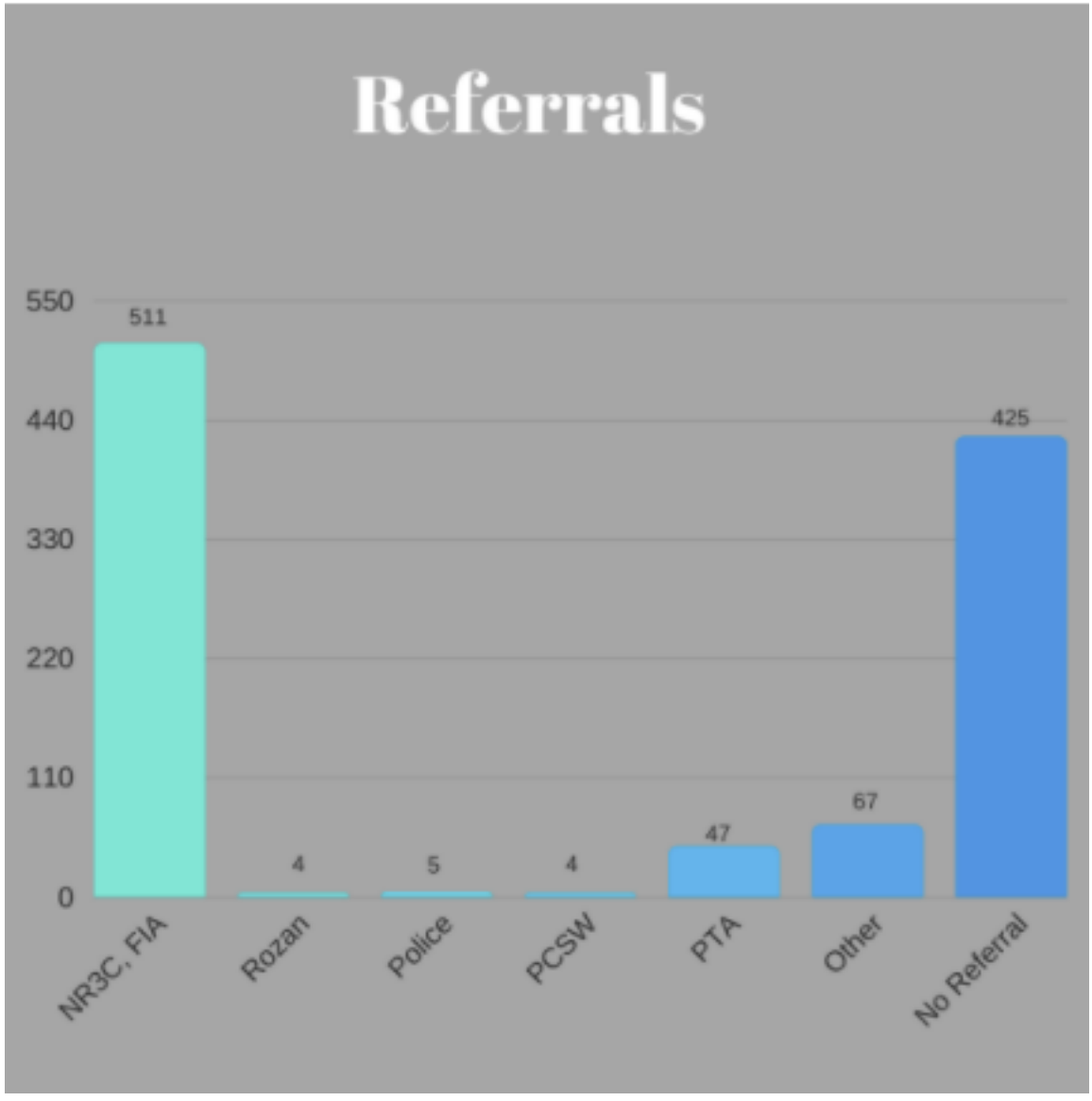

Figure 14: This data is based on the total number of individual cases, not number of total calls attended.

As is evident above, 48% of our cases are either fully or partially referred to the FIA, given that it is the designated agency under PECA. Once cases are referred to the NR3C, it becomes very difficult to follow up on them or track their progress given the lack of complaint service delivery mechanisms. It has been observed by the Cyber Harassment Helpline that the numbers provided by the NR3C (it's helpline and complaint cell) are often non-operational. In the event that a case is registered, the likelihood of it being converted into an FIR is very low and, furthermore, of the case making it to the prosecutorial stage is even lower.

NUMBER OF COMPLAINTS*	NUMBER OF INQUIRIES*	NUMBER OF FIRs*
12,339	1,623	232

Only 1.88% of complaints get to the FIR stage, largely due to the lack of resources and capacity of the NR3C. Thus, cases referred to the NR3C by the Helpline experience a plethora of obstacles.

Geographical Distribution:

In order to understand the geographical patterns of harassment cases and the outreach of the Helpline itself, information regarding the city or area of residence is collected. Keeping in line with the data privacy of Helpline, the callers are neither required to provide their address, nor does the Helpline Staff collect it.

A majority of the cases received by the Helpline were from Punjab (50%), the most populous province in Pakistan.

** Source: The National Response Center for Cyber Crime (NR3C), FIA, from 18th August, 2016 to November, 2017.*

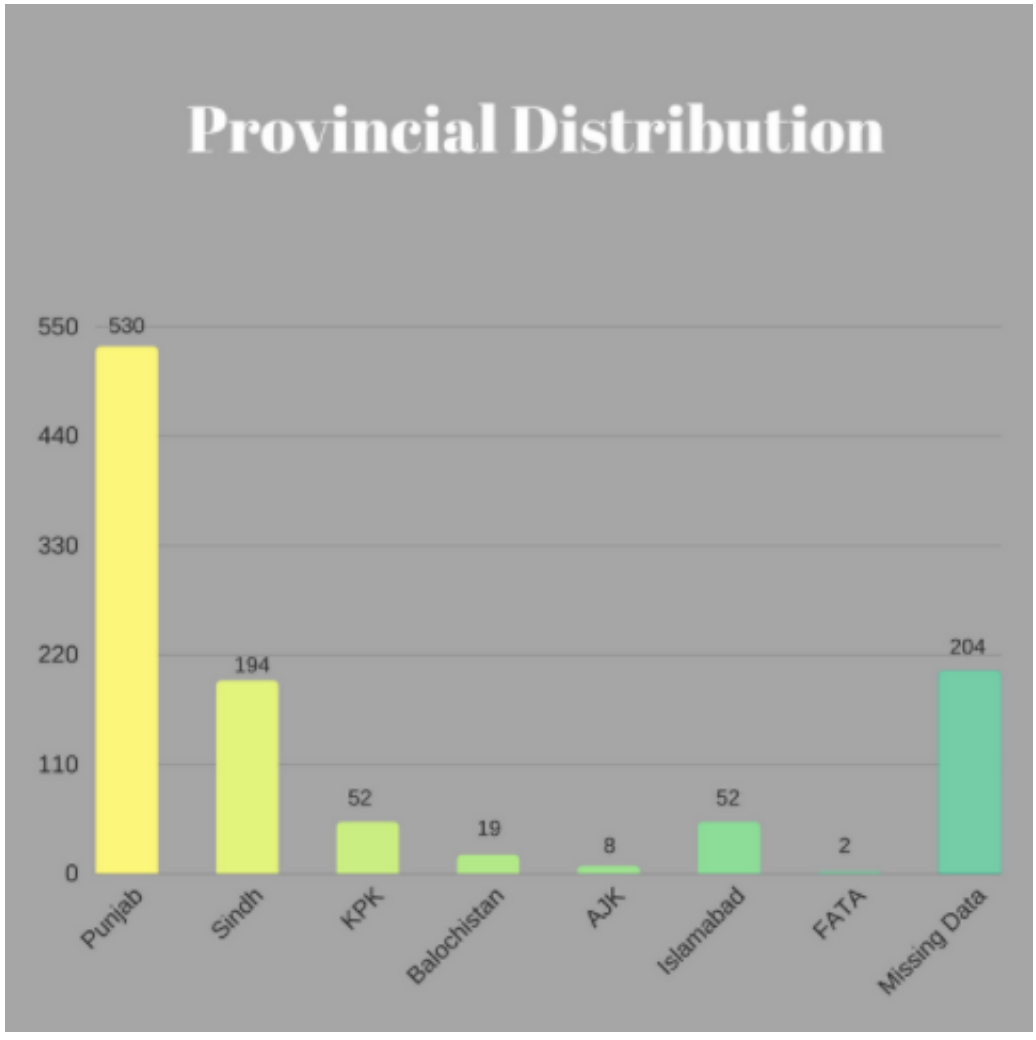

Figure 15: This distribution is based on the number of individual cases. The significant number of missing data is in cases where either it was deemed inappropriate to ask for location data, or when the complainant refused to provide it.

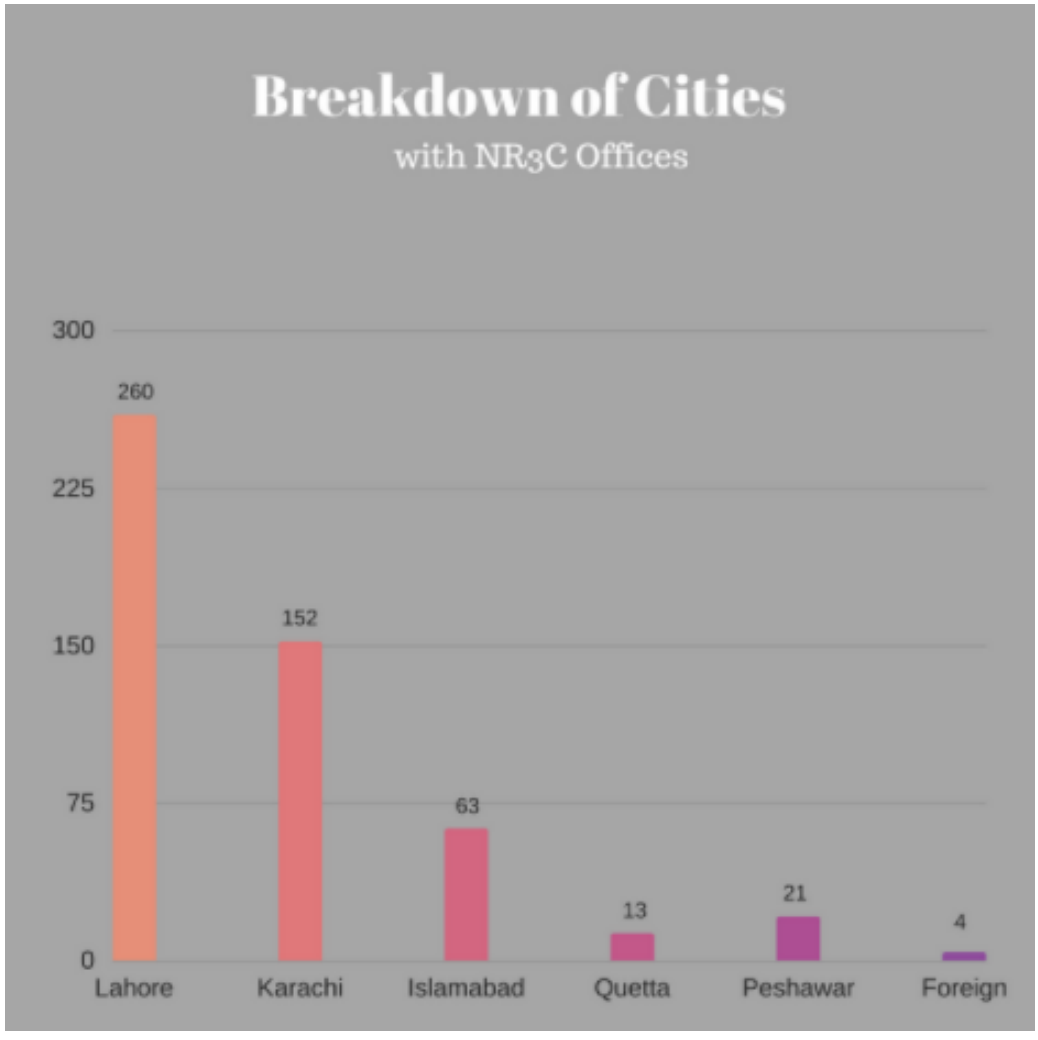

Figure 16: This data is based on the number of individual cases.

(In)accessibility to FIA's Offices:

Access to LEAs is one of the most important determinants of the functioning criminal justice system. The fact that the FIA's National Response Centres for Cyber Crime (NR3C) offices are only located in Islamabad, Peshawar, Quetta, Karachi and Lahore is a major impediment to reporting cyber harassment, and cyber crime in general. The FIA's procedure for reporting requires that the complainant travel to the NR3C's office in person and register their case in order to commence legal proceedings. As mentioned above, 48% of the cases the Helpline receives come under the domain of the FIA.

Figure 16 below shows the number of calls received from cities with offices of the NR3C ("Cities with NR3C") in comparison to the number of calls from other cities and areas ("other cities") where the cyber crime offices are not located. If callers from "other cities" want to pursue a legal case they will have to travel to their nearest NR3C, located in a different city, simply to lodge a complaint. Furthermore, this journey will have to be made regularly if they chose to follow up on the case. We received around 57% cases from areas with no offices of the NR3C, adding a layer of inaccessibility to the entire process.

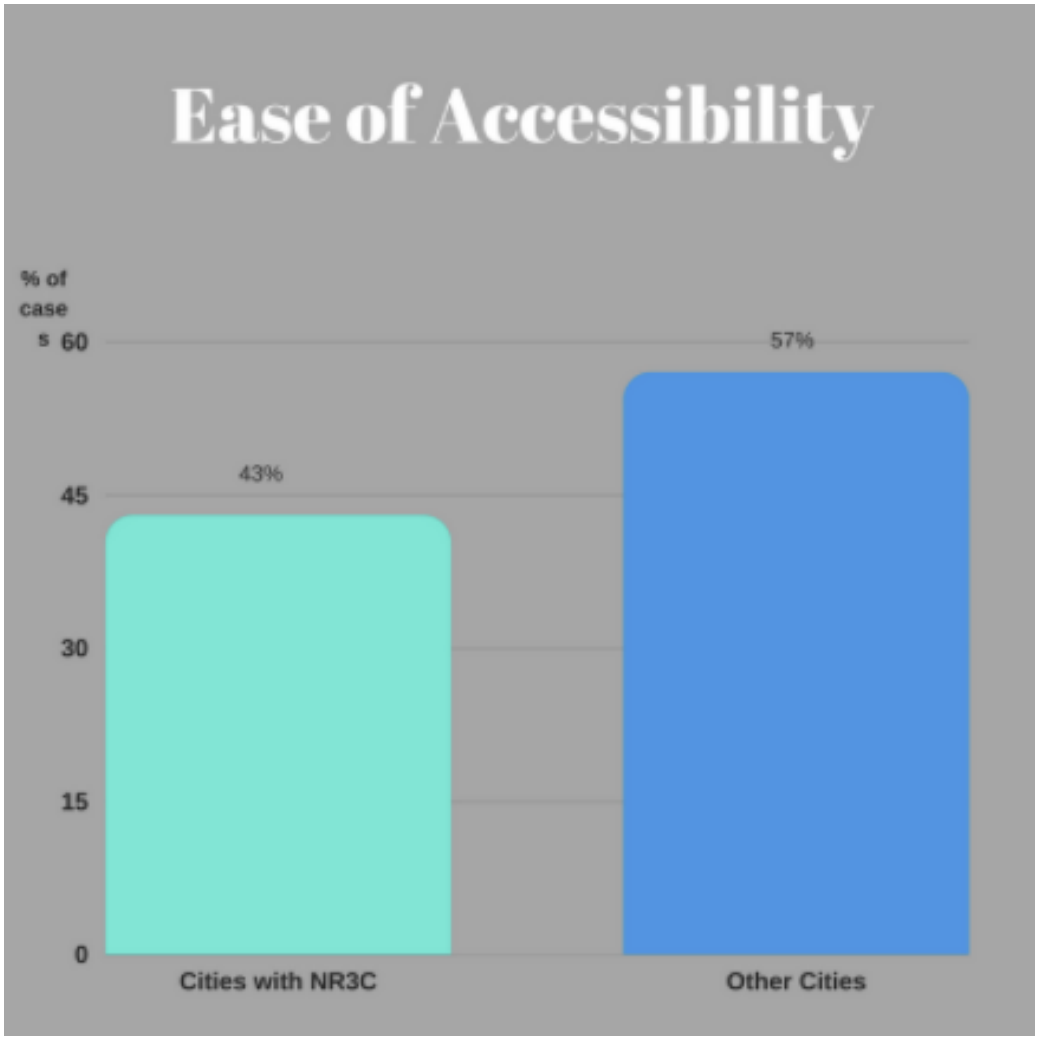

Figure 17: This data is based on individual cases, not the total number of calls.

Age Distribution:

A majority of our callers were between the ages of 20 to 30 years (61%), mostly in their early 20s. Read with the gender ratio discussed earlier, it can be extrapolated that the most vulnerable demographic in terms of online harassment is young women. It is also interesting to note that 5% of the complainants were under the age of 18, which is below the age of majority and consent, and raises a number of legal questions and concerns regarding child pornography (made illegal under section 22 of PECA).

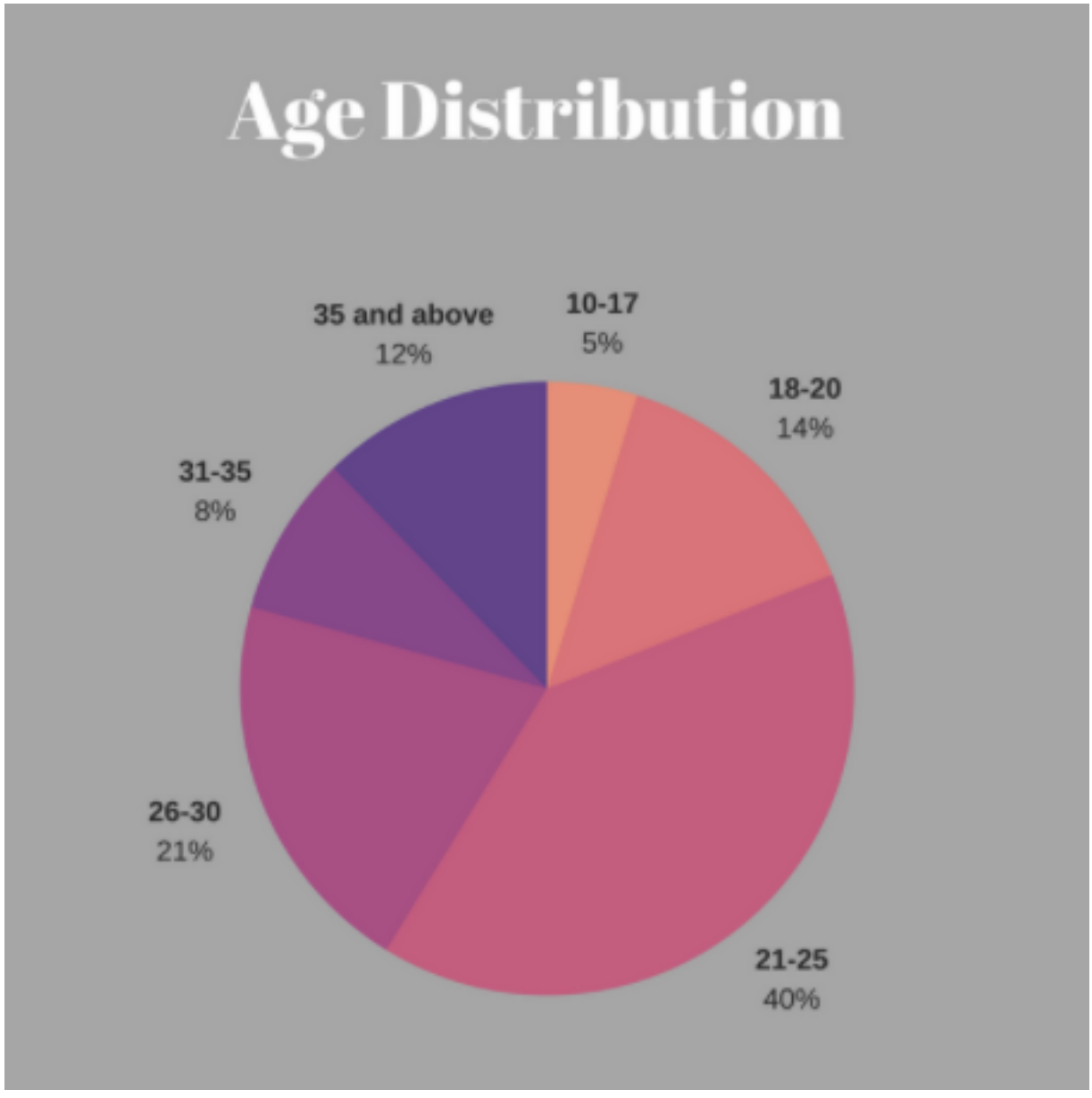

Figure 18: This data is based on individual cases, not the total number of calls.

Mental Health:

Since the six-month report, the Helpline has been recording the impact of psychological data on the basis of mental health indicators developed by the mental health counsellor. These indicators are not recorded on every call and it is only done so when the caller is exhibiting signs of mental distress that fall within the predefined categories. Furthermore, DRF has conducted a descriptive and psychological review of data gathered through calls to understand effects of cyber harassment on mental health. Jannat Fazal from DRF has explored the mental health implications of online harassment in an abstract titled "Online harassment: a retrospective review of records".[11]

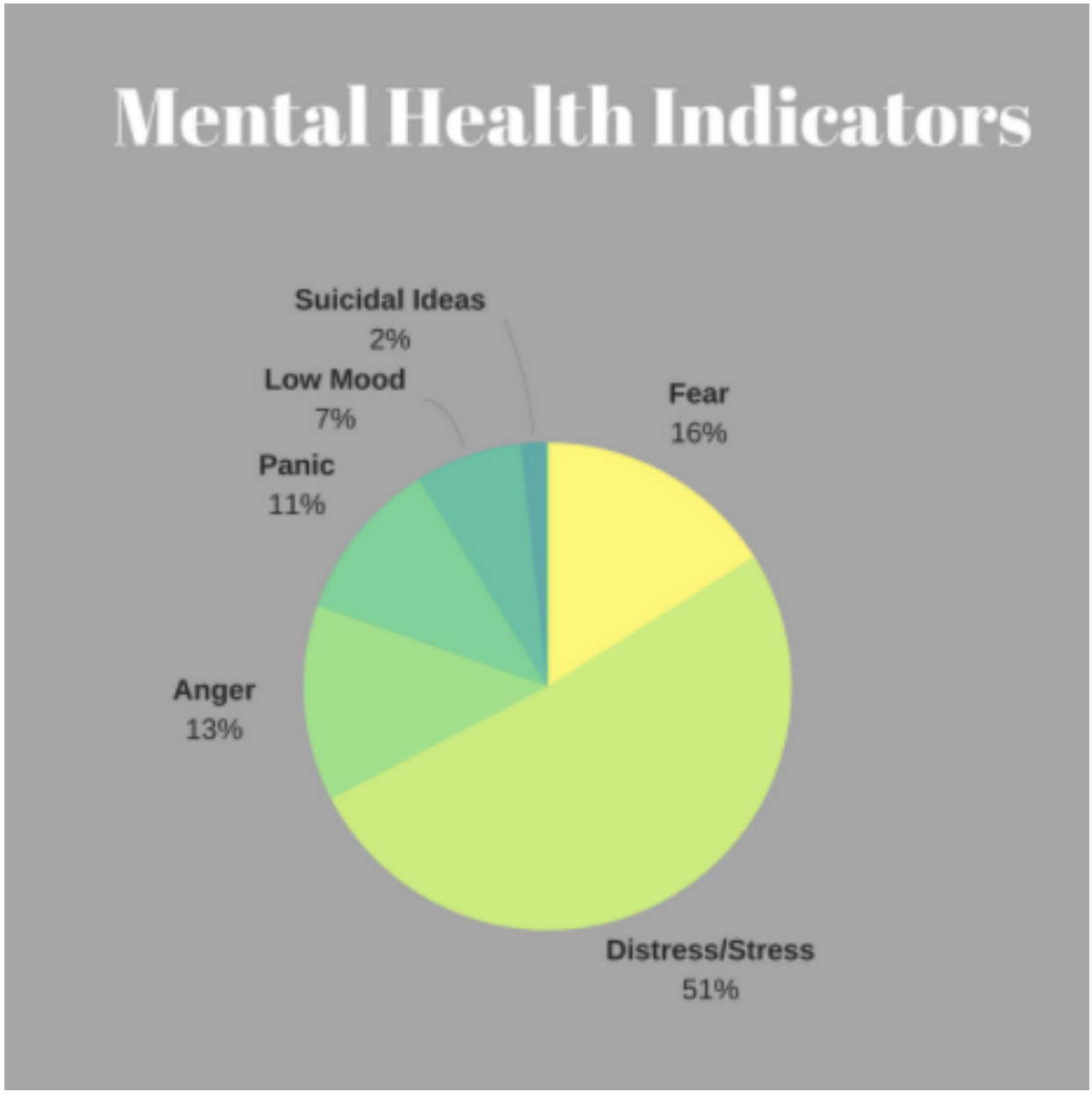

Figure 19: This data is based on a small sample of calls where psychological data was recorded.

[11] *"Online harassment: a retrospective review of records", Médecins Sans Frontières (MSF) Scientific Day South Asia 2017,* https://f1000research.com/slides/6-785.

THE FUTURE:
ROADMAP FOR HELPLINE

The first year of the Helpline's operations was marked by defining structures and processes to streamline its work. The next year aims to capitalize on expansion and meaningful outreach by consolidating existing structures and adopting them to ensure malleability to the local context.

The Helpline has met its goal of successfully launching its operations, regular reporting[12] and sustaining a consistent number of calls in its first one year. The Helpline now plans to expand its geographical reach and advocacy. The Helpline will conduct outreach in less urban settings to ensure that awareness about its services is not just restricted to major cities. Online harassment and violence is not solely an urban issue and as cases such as the Kohistan case show, women in these areas are even more vulnerable due to lack of institutional support.[13]

The Helpline wishes to establish a more robust referral mechanism with the law enforcement agencies to ensure timely registration of cases and speedy investigation.

In August 2017, we met our goal of expansion of the Helpline from five days a week to seven days (from 40 hours to 56 hours) to ensure greater access and flexibility for our callers.

On the advocacy front, DRF has used the data produced by the Helpline to push for reforms of reporting mechanisms and the organisations tasked with addressing online harassment. The Helpline wishes to build on this work to launch advocacy campaigns to ensure better implementation of laws. Over the next year, Helpline reports will be accompanied by policy briefs, which will use the data generated by the Helpline to suggest policy interventions. DRF envisions data and victim-led reform as part of the future work of the Helpline.

---

[12] *"Cyber Harassment Helpline: Six Month Report, December 2016 – May 2017", Digital Rights Foundation, https://digitalrightsfoundation.pk/wp-content/uploads/2017/07/Cyber-Harassment-Helpline-Six-Month-Report.pdf.*

[13] *Naveed Siddiqui, "Kohistan video case: Girls declared alive by SC had actually been killed, says Bari," Dawn, October 21, 2016, https://www.dawn.com/news/1291398.*

RECOMMENDATIONS:

Digital Rights Foundation wishes to use the data that it collects to enhance existing policy-making and institutional responses to online violence and harassment in Pakistan. Based on the data presented above and the experiences of our callers, we put forward the following recommendations:

1. **PECA Rules:** When drafting rules u/s 51 of the PECA, 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:** There has been an exponential growth in cyber crime cases at the NR3C over the years. According to the FIA's own 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-year period from 2017 to 2022, it means that the increase in resources should neither be limited to meet the current demand, nor the current rate of growth. 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 and means 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. Mechanisms of investigation need to catch up with substantive law. 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. 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.

4 **Regular reporting and performance review of the FIA:** DRF urges the FIA to fulfil its obligations u/s 53 and submit 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.

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 counselling 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.

8 **Privacy and Confidentiality:** One of the biggest barriers for reporting cases of cyber crime, particularly online harassment, to law enforcement is the fear of leaked information and 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.

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:** When cases involve both online and offline crimes, complainants receive contradictory advice regarding the overlapping jurisdiction of the police and NR3C. DRF recommends that channels of communication between police stations and cyber crime stations be established and strengthen to ensure a reliable and litigant-friendly referral system.

11 **Psychological needs:** 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.

12 **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.

13 **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 behaviour 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.

14 **Check on performance of investigators and prosecutors:** Internal mechanisms should be in place to review the performance of investigators and prosecutors. The incompetence and insensitive behaviour of these officers towards the complainant can lead to 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.

15 **Greater technical expertise:** Several complaints to the NR3C experience 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 cyber crime, 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.

16 **Training for judges on cyber crime law, internet governance and online harassment:** Internet governance and cyber crime 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 cyber crime, but that they also fundamentally misunderstand the governance and infrastructure of the internet itself, which leads to bad jurisprudence and, at times, "unimplementable" orders.

17 **Collaboration with organizations working on online harassment:** 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.

www.digitalrightsfoundation.pk

/DigitalRightsFoundation

@DigitalRightsPK

Digital
RightsFoundation

"KNOW YOUR RIGHTS"