CYBER HARASSMENT HELPLINE

Bi-Annual Report
December, 2016 – May, 2018

0800-39393

Everyday
9am-5pm

DRF

DigitalRightsFoundation
"KNOW YOUR RIGHTS"

About

Digital Rights Foundation (DRF) is a feminist, not-for-profit organisation based in Pakistan working on digital freedoms. DRF 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 such a healthy and productive environment that would eventually help not only women, but the world at large.

Acknowledgments

We want to dedicate this report to the incredible women who come forward with their stories of harassment every day, both publicly and privately. Our Helpline strives to make this a safe space for women who talk about their traumas. We want to let them know their stories are valid, and they always have a place that believes in them.
The Helpline Team would like to thank everyone who has stepped up to support its operations and assist in spreading the word.
This report is also dedicated to the key staff member of the Helpline, Hyra Basit, who is leaving us to pursue her studies. She brought incredible empathy and dedication to her work. We will miss you dearly, you are irreplaceable.

Contents

Background 1
About: Pakistan's first Cyber Harassment Helpline 5
Helpline Data:
- Understanding cyber harassment in Pakistan 7
- Total Number of Cases .....
- Volume of Calls .....
- Gender 9
- Types of Cases 11
- Platforms 15
- Referrals 16
- Geographical Distribution 18
- Accessibility to FIA's Offices 19
- Age Distribution 20
- Services Provided 21

Recommendations 22

Background:
Online Harassment

Digital Rights Foundation (DRF) is a pioneering organization in Pakistan working on issues of online harassment, technology and gender in terms of research, advocacy and support for victims. Online harassment and related threats 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.

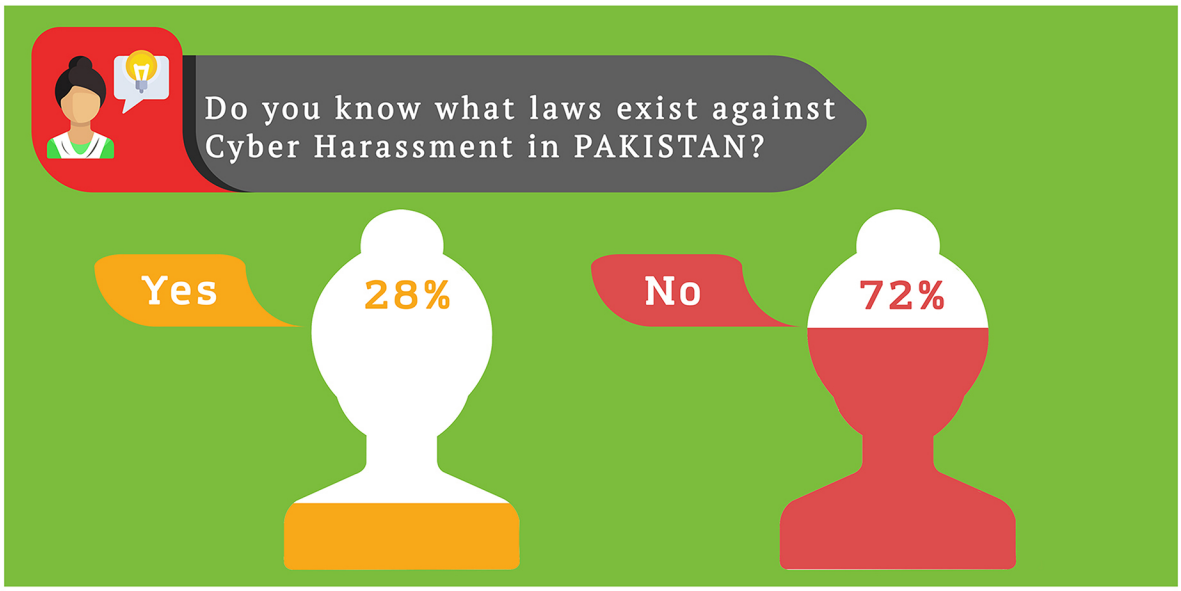


Figure 1: Level of awareness regarding online harassment laws in Pakistan.

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. 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.

---

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.

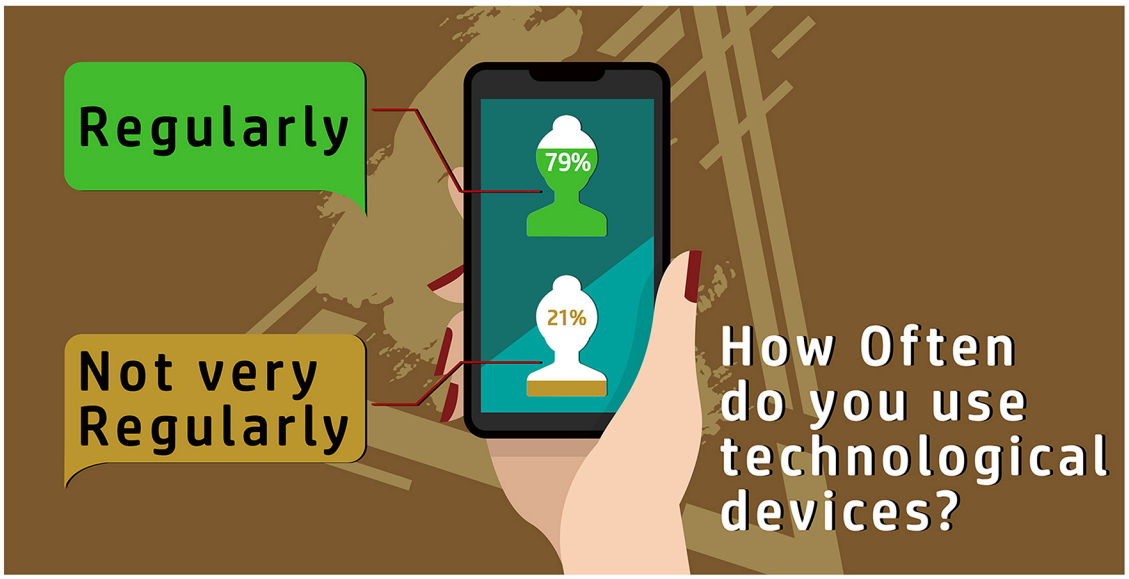


Figure 2: Frequency of technological use among young Pakistani women.

However, the use of these technologies is gendered and informed by the user's positionality. Young women are much more likely to be self-censored online and to be harassed online. This makes them more vulnerable in online spaces, along with religious minorities and activists in Pakistan.

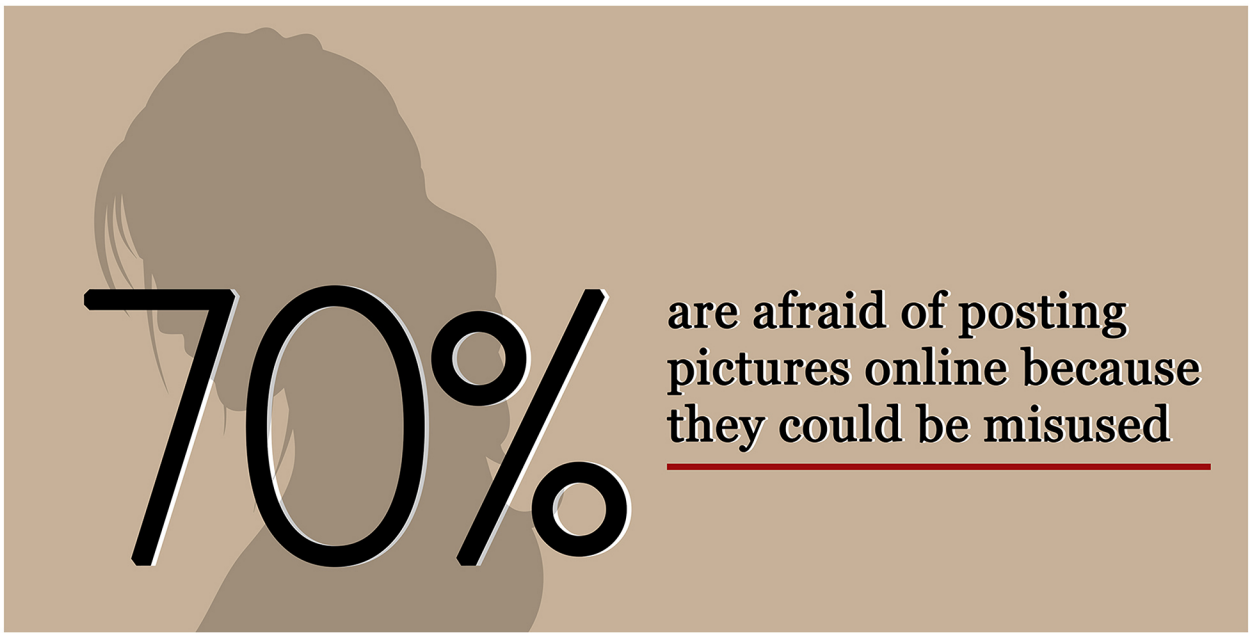


Figure 3: Measuring the proportion of women who hesitate before posting online.

---

3 Note 1.
4 Note 1.

Figure 4: Measuring the proportion of women harassed online.

DRF also observed a serious gap in addressing online harassment in individual cases. Furthermore, several women were reaching out to DRF regarding their cases of online violence and harassment, which led us to conclude that there was a need to streamline our efforts and institutionalize the process of helpline individual complainants.

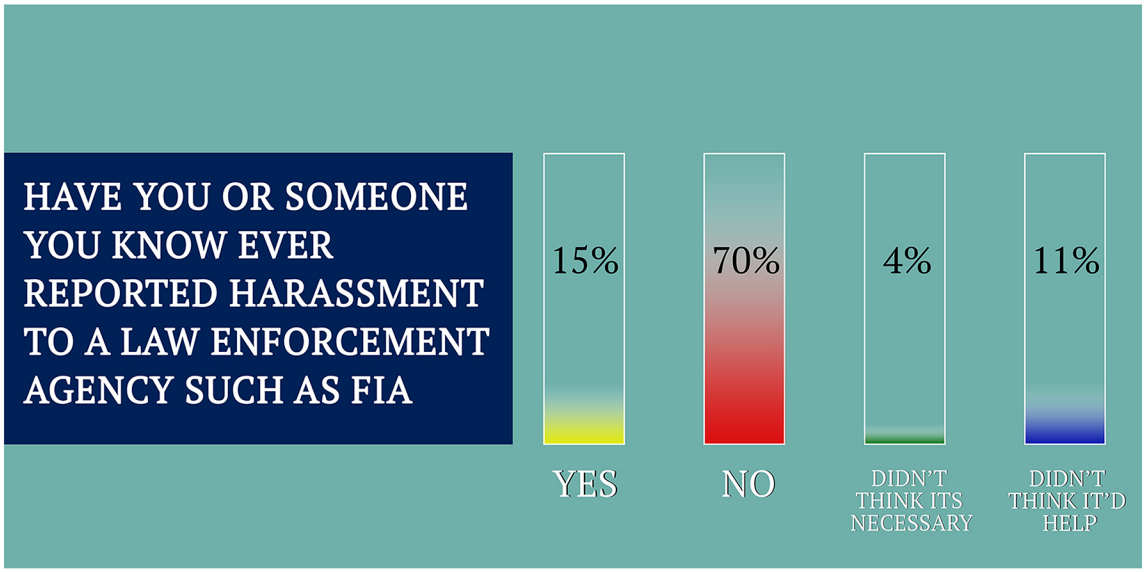


Figure 5: Measuring rate of reporting online harassment among women.

The Helpline seeks to address these gaps in the system and problems that women face 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 a high-quality service.

---

5 Note 1.
6 Note 1.

Figure 6: Reasons for not reporting online harassment.

7 Note 1.

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, and trained 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.

The soft launch of the Helpline was on November 28, 2016 and it 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. This report was delayed due to some unforeseen technical and staffing issues.

& Goals Objectives of the Helpline

The goal of the Helpline is to make online spaces safe for all, especially women. We see online harassment as the leading factor of insecurity in digital spaces. Thus the Cyber Harassment Helpline seeks to provide Pakistani women with the necessary tools to tackle online harassment, taking into account the specific needs of women and marginalized communities.

By way of clarification, the Helpline does not seek to replicate the efforts of law enforcement and investigative agencies; in fact, our aim is to complement those institutions and the work that they perform. **Thus, the Helpline does not investigate or prosecute cyber crimes; it 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 accountable and track their progress once cases have been referred to them.

Objectives for Cyber Harassment Helpline:

1. Increase awareness of digital security among complainants.
2. Provide a safe, judgement-free, gender-sensitive and confidential environment for victims to share their experiences of online harassment.
3. Provide direct and quality mental health counselling to victims who indicate signs of psychological distress.
4. Awareness regarding complainants' digital rights and legal advice to complainants regarding online harassment law, procedure of filing a criminal complaint and setting realistic expectations of legal remedy.
5. 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.
6. Collect non-personally identifiable information to be used for purposes of advocacy and research.
7. Produce and publish regular operational and transparency public reports.

Success Indicators

1. Satisfaction of individual callers.
2. Development of robust protocols and policies for the Helpline to ensure data and caller security.
3. Maintain a steady number of calls throughout the year.
4. Outreach outside urban centers.
5. Development of a comprehensive and responsive referral system in partnership with various social media companies, service delivery, civil society and government organizations.

Helpline Data: Understanding cyber harassment in Pakistan through numbers

The primary channel for communication for the Helpline is the toll-free number; however, the Support Staff also entertains complaints over email and Facebook inbox. The Helpline has received 1,908 complaints in the form of calls in its first year and a half, from December 1, 2016 to May 30, 2018.

Volume of Calls

In its first year, the Cyber Harassment Helpline provided services to **1,908 calls** on its toll-free number. Out of the total number of 1,908 calls, were first time callers and 420 were follow-up calls from people who were either updating their assigned officer about their case or seeking additional information/assistance. We encourage our callers to keep in touch with the Helpline staff, however since the Helpline does not store phone numbers we do not call back in non-emergency situations.

Total calls	1908
Total New call (Individual cases)	1488
Total Follow-up Calls	420

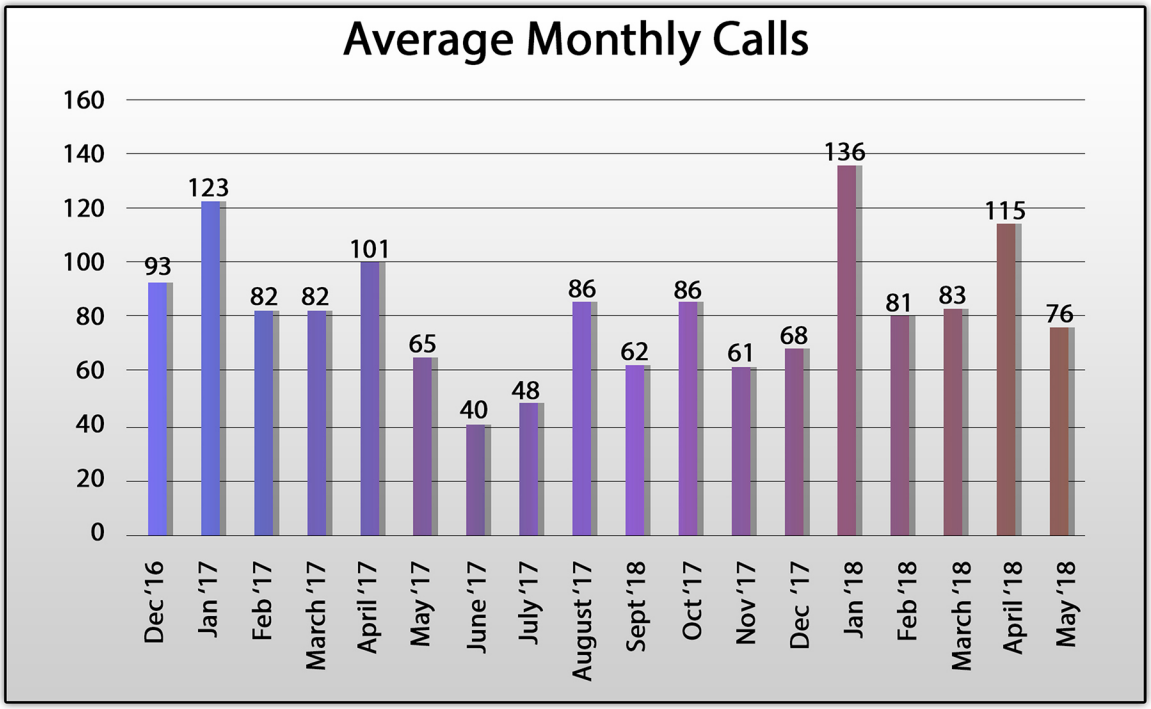


Figure 7: This data is based on the total number of calls attended (1908), not number of individual cases.

Average Number Of Calls

83

calls each month on the Cyber Harassment Helpline

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

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.

Gender Ratio

Online harassment is experienced primarily by women, an observation that is backed up by data provided by the FIA; **3,252 out of 12,339** complaints (26.36%) for cyber crime at the National Response Center for Cyber Crime (NR3C) were by female complainants. Furthermore, as per the FIA's performance report of the first quarter of 2018, **90%** of the victims in cases reported to the Cybercrime Circle in Lahore were women. As of April 2018, "2,753 cases of cyber harassment and blackmail that are registered in the [Punjab] cell."

We, too, collect gender segregated data to gauge the specifically gendered impact of online harassment. 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." We understand the bifurcation of data along the binary of male and female is exclusionary of other non-binary and gender non-conforming individuals, and while it is our practice not to assume gender unless the caller identifies as such—nevertheless given the fact that none of our callers have identified as non-binary is a product of power dynamics. Creating a safe space for our callers is a process and we hope to move further in creating a truly gender inclusive and welcoming space in the future.

Based on the number of cases where data was available, 63% of our callers were women and the remaining 37% were men. It is important to remember that this is not indicative of the overall cases of harassment that occur in Pakistan, rather the number of cases reported to Digital Rights Foundation.

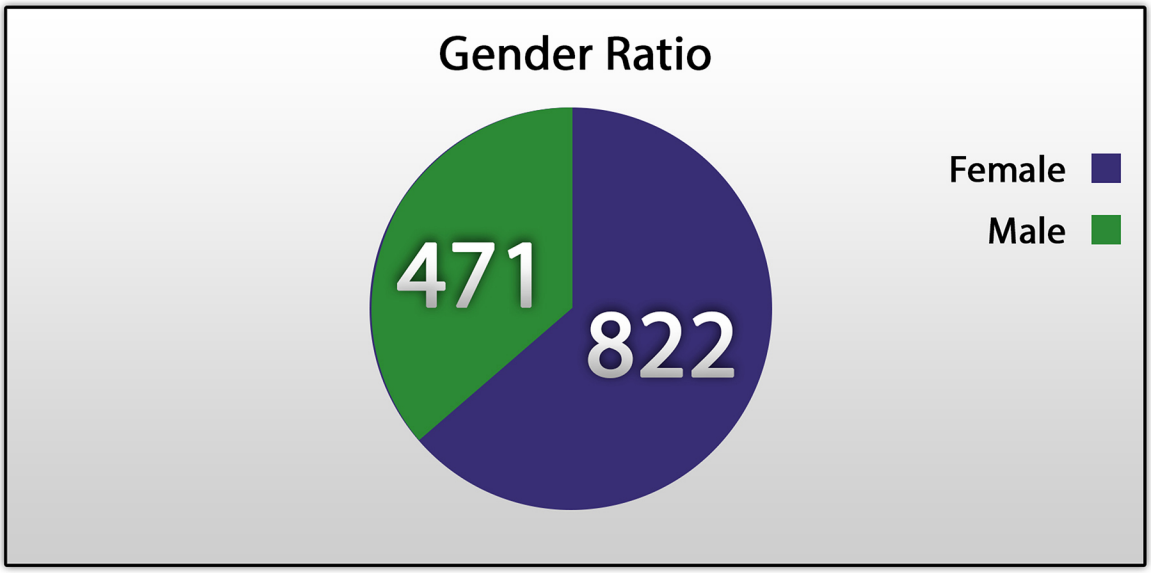


Figure 8: This data is derived from the total number of individual cases (1488), not the total number of calls. The number of female callers were 822 and male callers were 471. A small discrepancy of 195 cases exists due the inability to confirm information given the sensitive nature of certain calls.

1052 (70.6%) of our total callers have been categorized as "self", i.e. calling about their own case. Thus, the gender-related data needs to be contextualised further to account for the callers who were calling on behalf of someone else, thus creating a disparity between the gender of the caller and the victim. In order to account for these situations we provide the "Gender Breakdown" data.

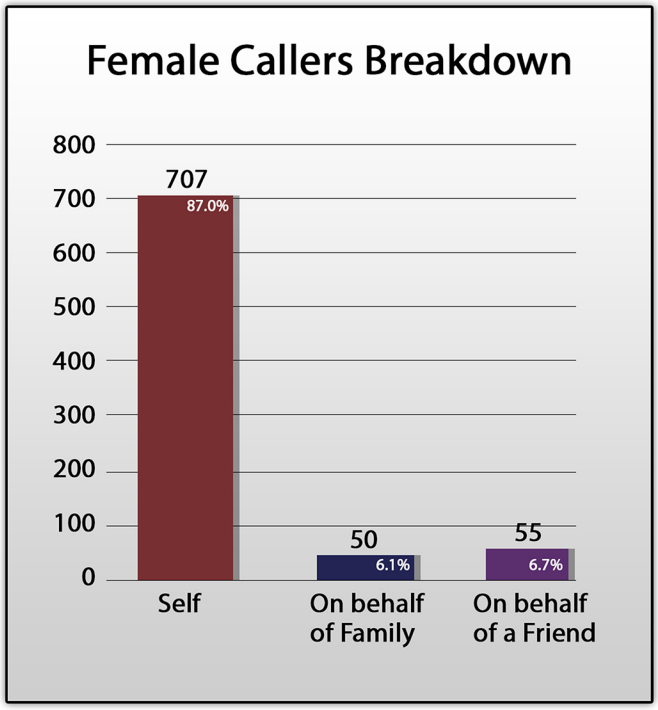


Figure 9: This data is based on the total number of individual cases.

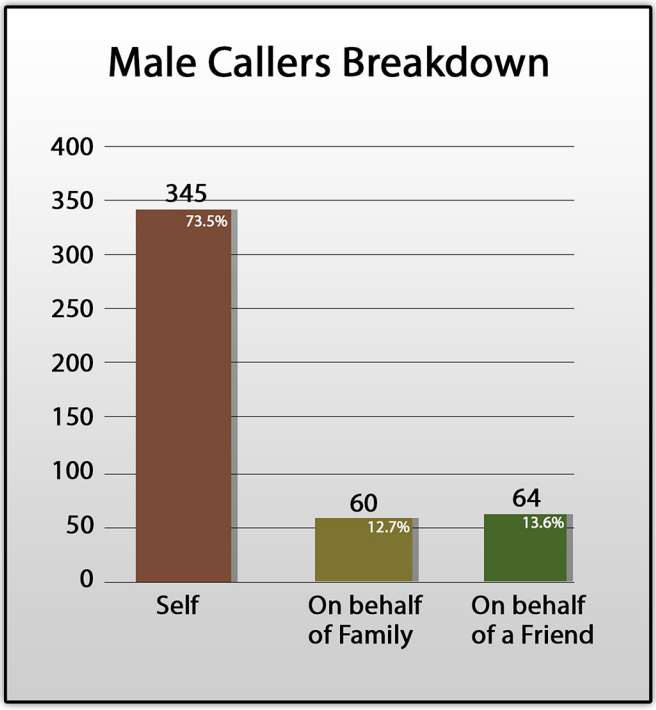


Figure 10: This data is based on the total number of individual cases.

It is apparent from the data that 87% of female callers are calling regarding their own complaint, while only 73% of male callers were calling regarding their own case. There is reluctance on part of some women to call on their own behalf, and in cases where a man is willing to take the lead, there is a preference of letting them speak to Helpline representatives. This is also reflected in many complainants' desire to have a male friend or family member approach the law enforcement authorities as well.

---

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

10 Warda Imran, "Of consent and copyrights: Women lodge 90% complaints in FIA Cybercrime Circle," The Express Tribune, April 9, 2018, https://tribune.com.pk/story/1681027/1-consent-copyrights-women-lodge-90-complaints-fia-cybercrime-circle/.

11 Note 10.

12 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.

Types of Harassment 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 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 for theft.

Unsolicited Contact:

Unsolicited contact involves unwanted and repeated calls and messages by the accused/abuser, which may include spam, repeated requests for contact, personalised 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 and 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 target 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 target 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 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.

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.

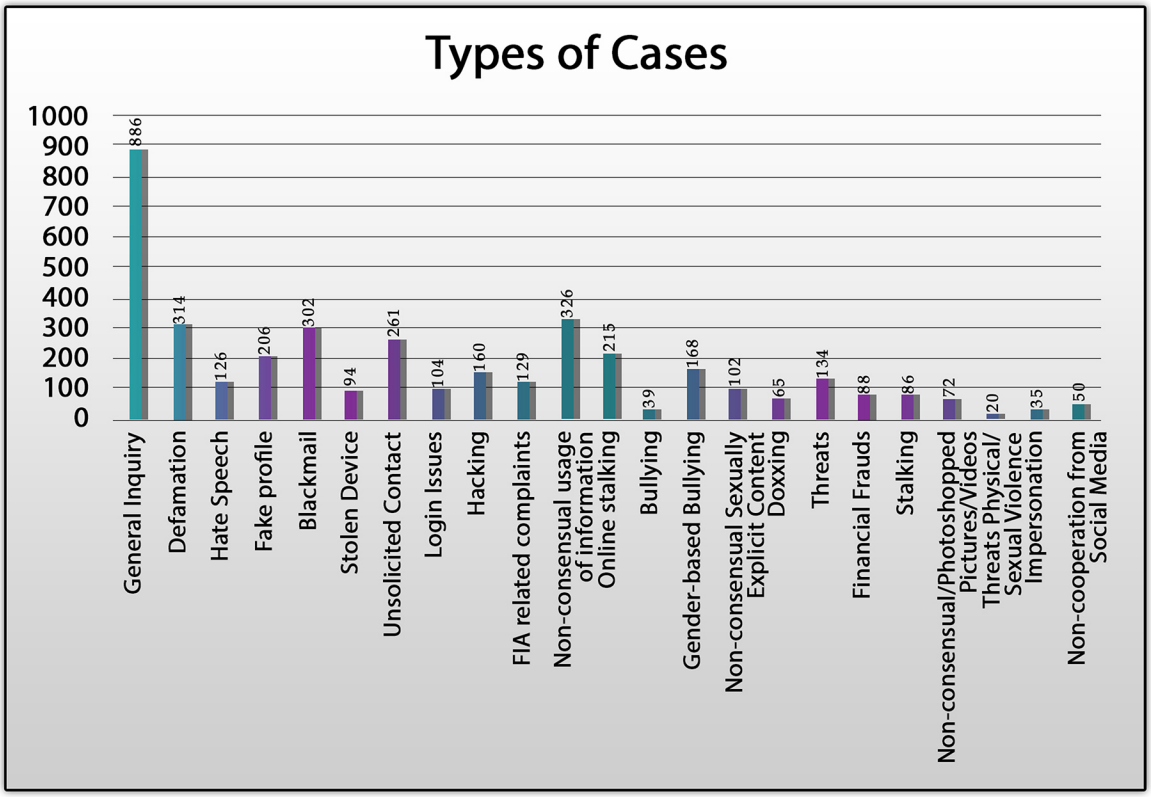


Figure 11: This data is based on the total number of cases. Keep in mind that some callers reported more than one type of complaint. The Helpline Support Staff categorized the nature of the complaint as "secondary" and "primary" according to the facts of each individual case.

It is clear that a majority of the cases related to defamation, blackmailing, unsolicited contact and fake profiles. In the last six months, the Helpline has experienced an uptake in calls relating to mobile-based scams that prey on the trust of individuals. One of the most common types of such scams involves 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 the Pakistan Army, government departments such as the Benazir Welfare Programme and telecommunication companies.

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 12 (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 (466 complaints)—43% of our callers experience harassment on Facebook.

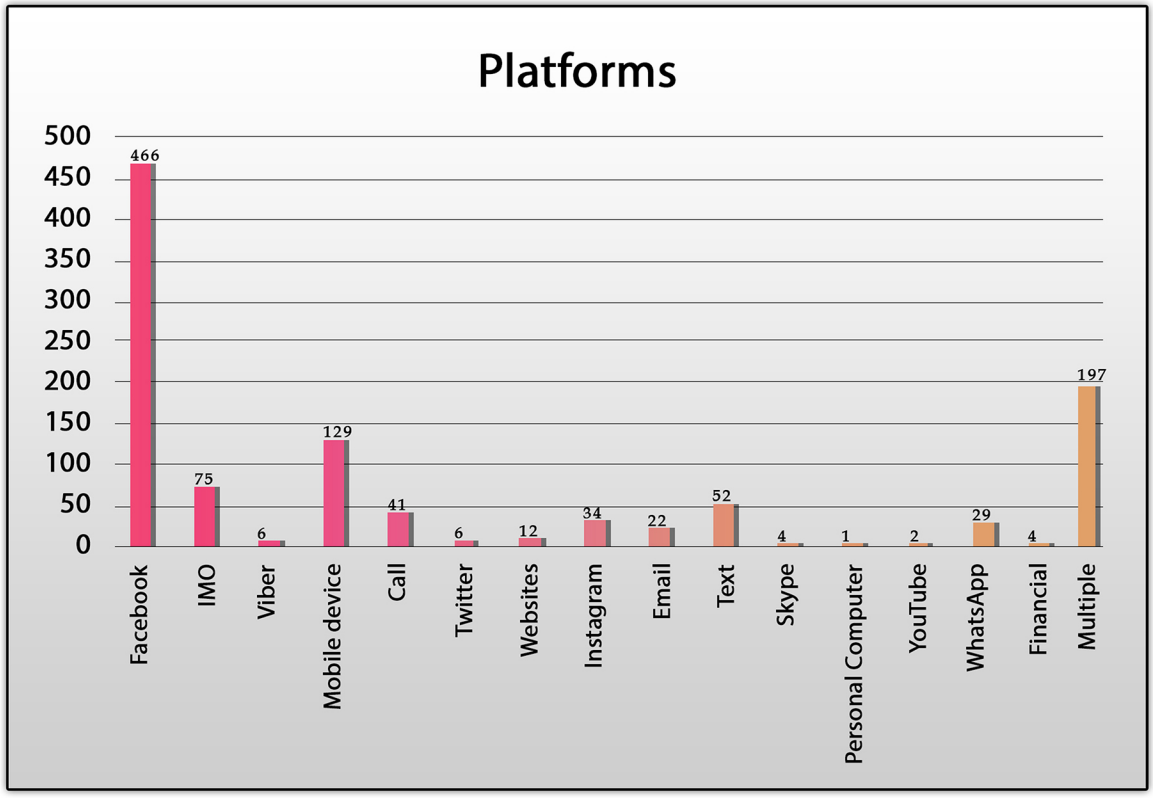


Figure 12: This data is based on the total number of individual case handled by the Helpline. There is a discrepancy of 408 cases as this category of data was not adequately and systematically obtained in the first month of operations (December).

Referrals

3.2% of complainants mentioned the FIA as part of their complaint to the Helpline and many others wished to file a complaint against their harassers. 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. The Helpline Staff referred 769 cases to outside organisations and partners.

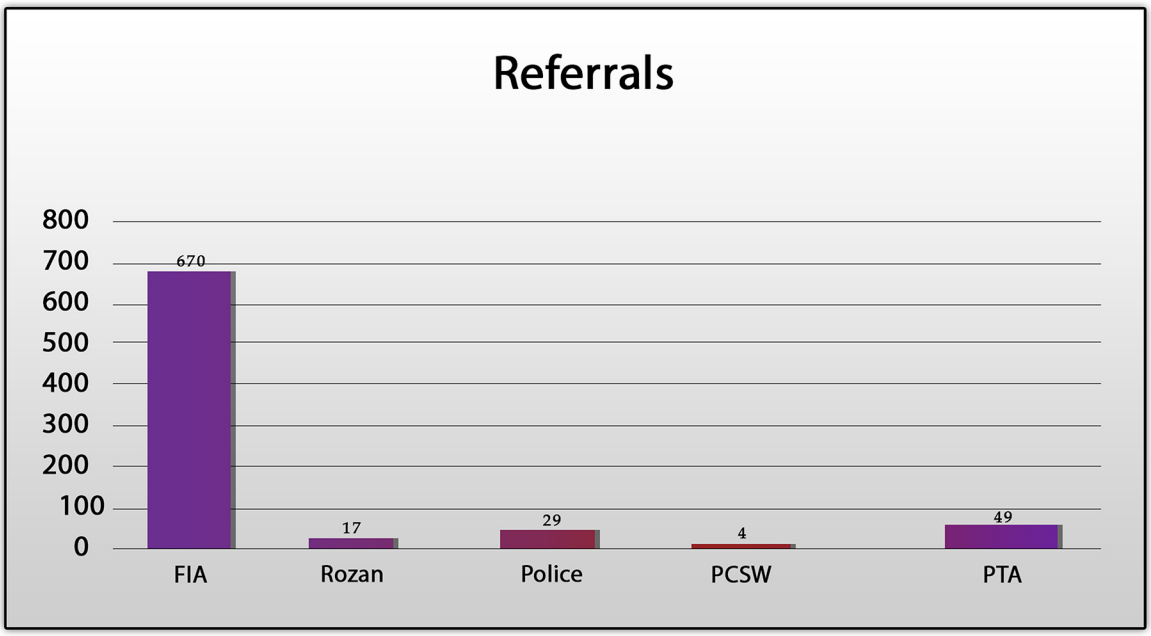


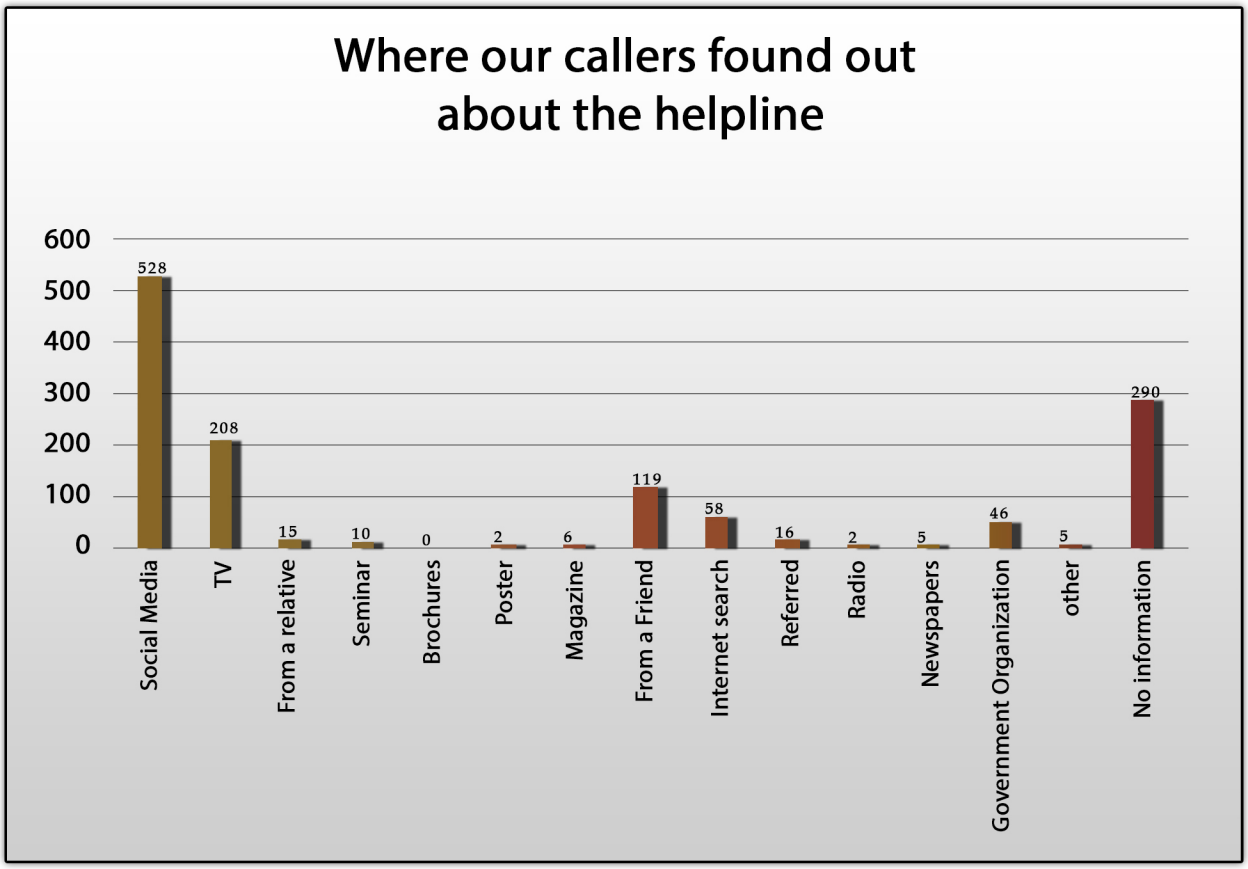
Figure 13: This data is based on the total number of individual cases, not number of total calls attended.

As it is evident above, 45% 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.

Complaints recieved by FIA.

No. of Complaints*	No. of Inquiries*	No. 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 (54%), the most populous province in Pakistan.

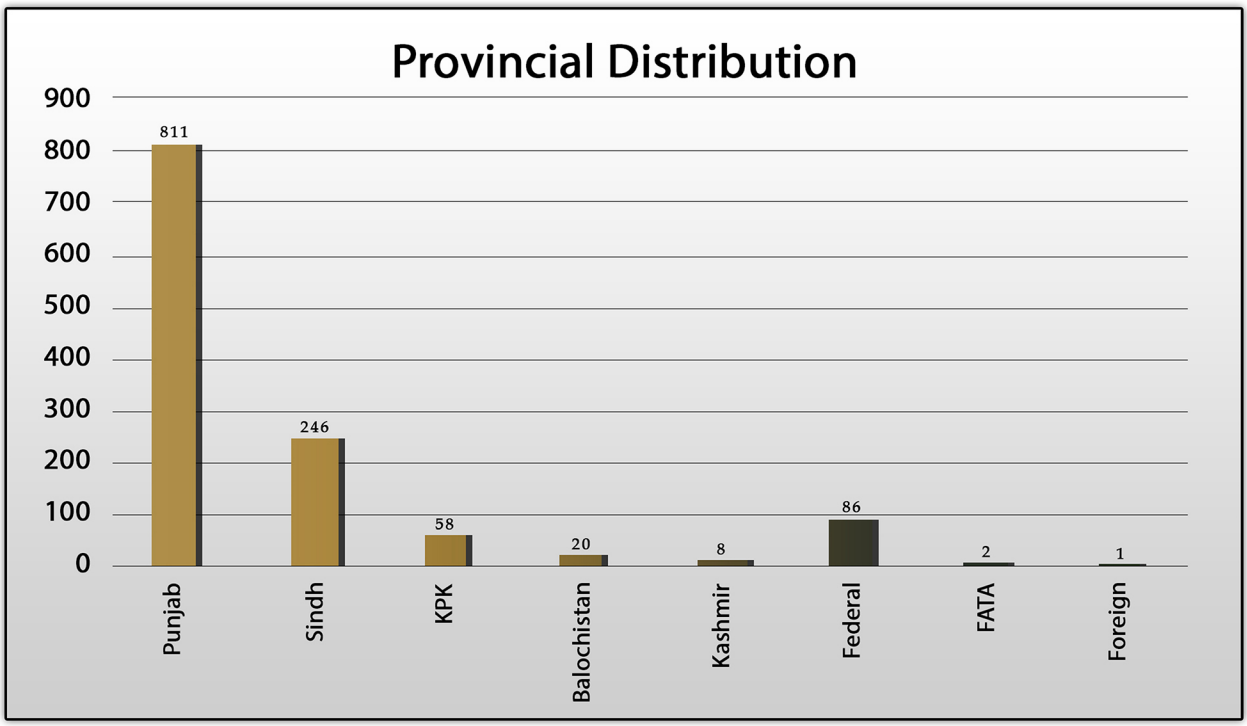


Figure 14: This distribution is based on the number of individual cases. The significant number of missing data is in cases where either it was deemed inappropriate to ask for location data, or when the complainant refused to provide it.

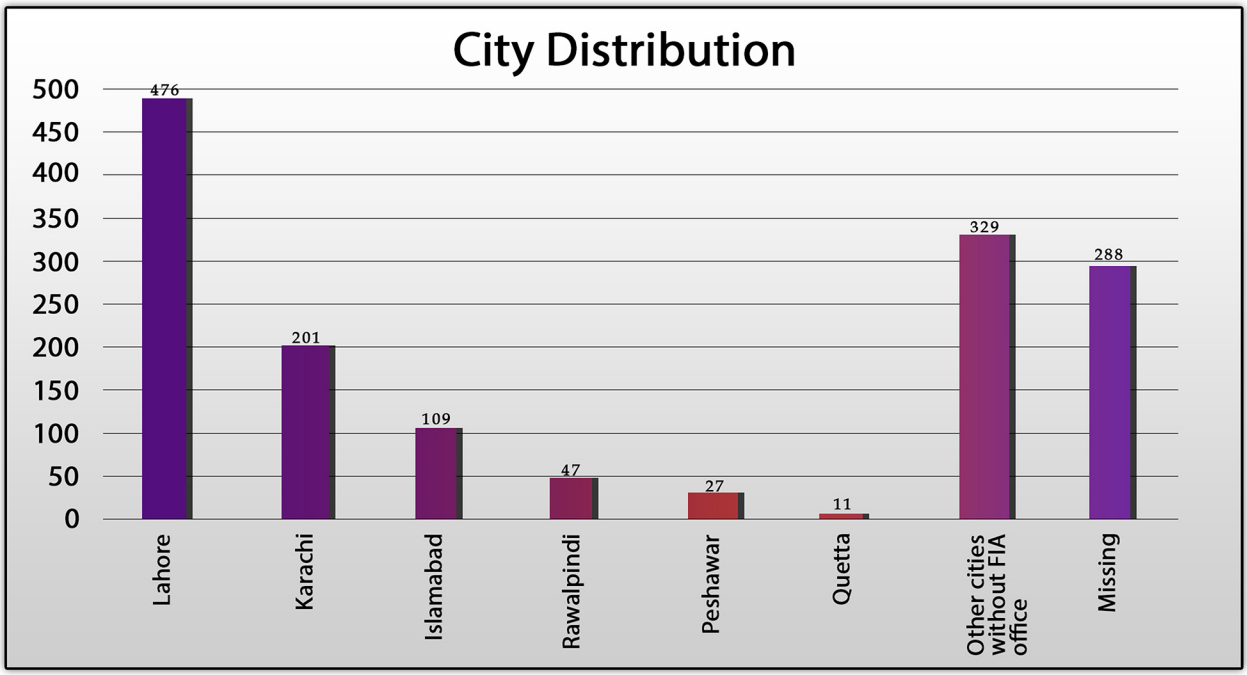


Figure 15: This data is based on the number of individual cases.

(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, 45% 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 choose to follow up on the case. We received around 22% cases from areas with no offices of the NR3C, adding a layer of inaccessibility to the entire process.

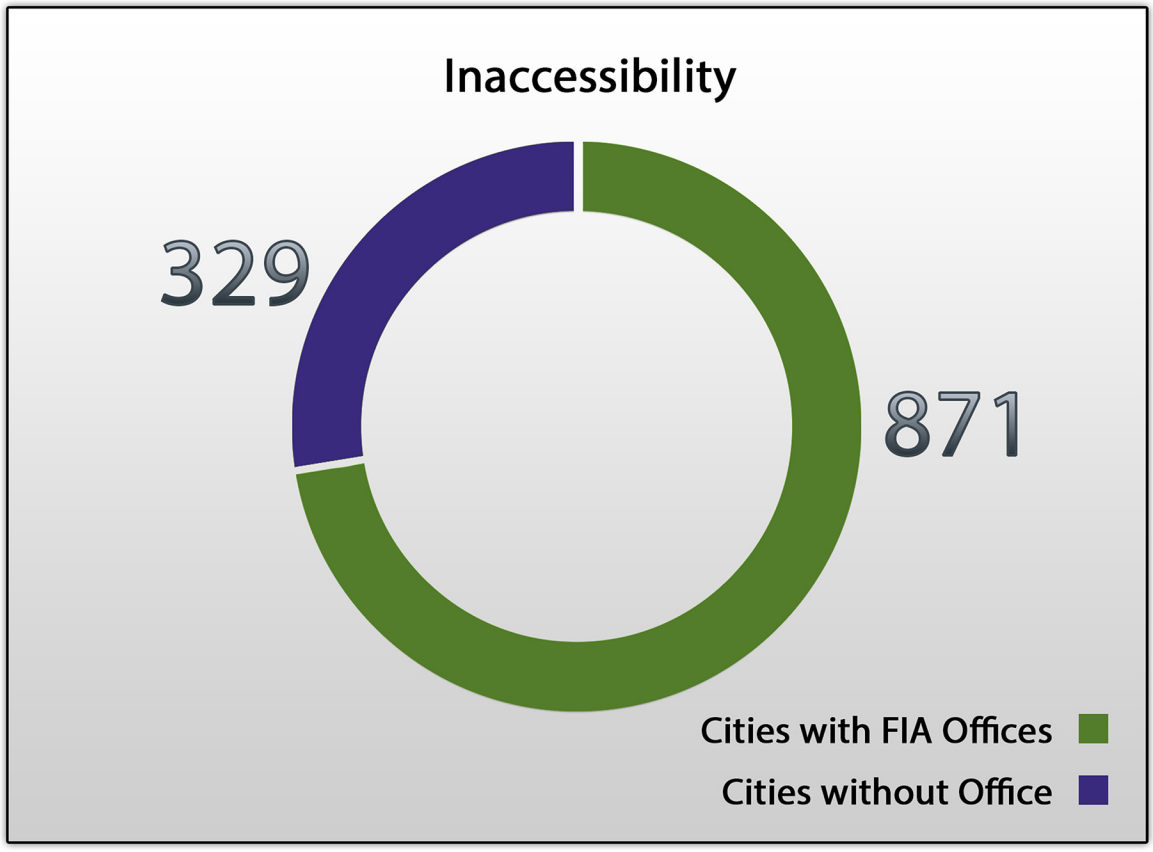


Figure 16: This data is based on individual cases, not the total number of calls.

Age Distribution

A majority of our callers were between the ages of 21 to 25 years (39.5%). 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 4.6% 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).

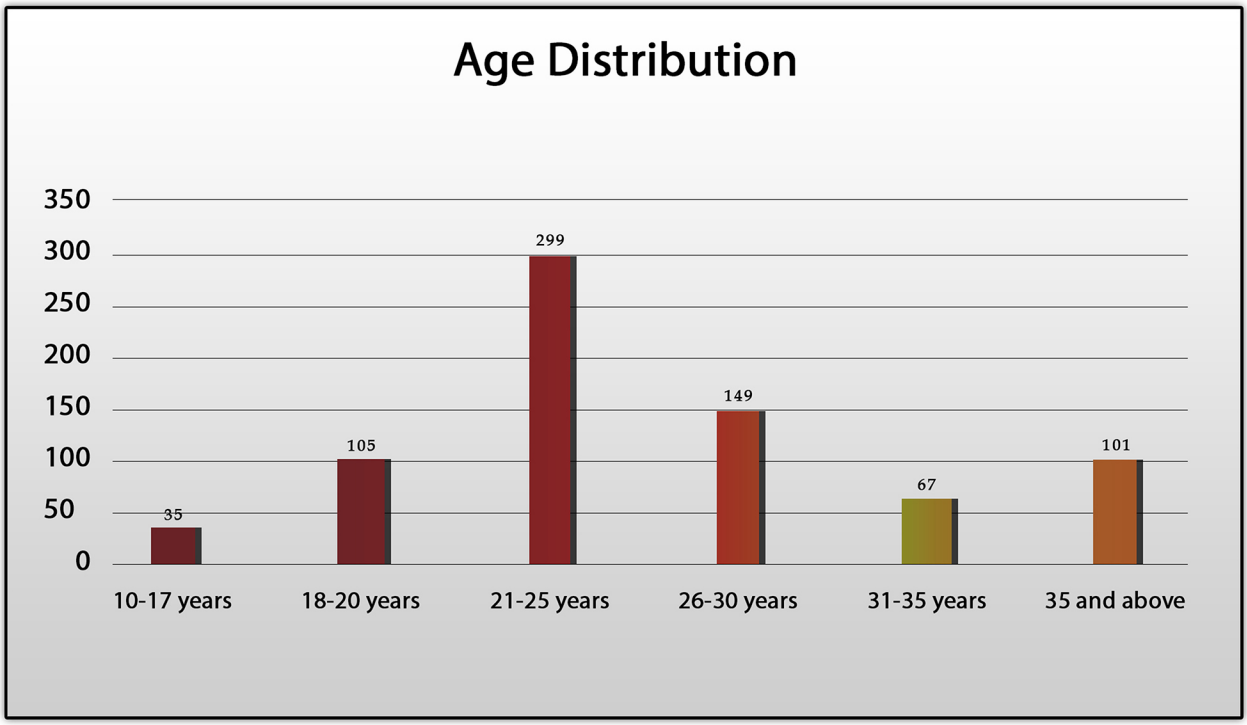


Figure 17: This data is based on individual cases, not the total number of calls. Since data regarding age distribution was gathered after 7 months of operations, the percentage taken a proportion of the number of cases where data was collected (756) rather than the total number of individual cases.

Type of Services Provided

As mentioned above, the Cyber Harassment Helpline provides legal advice, digital security support and mental health counselling. The following is a breakdown of the services provided on cases.

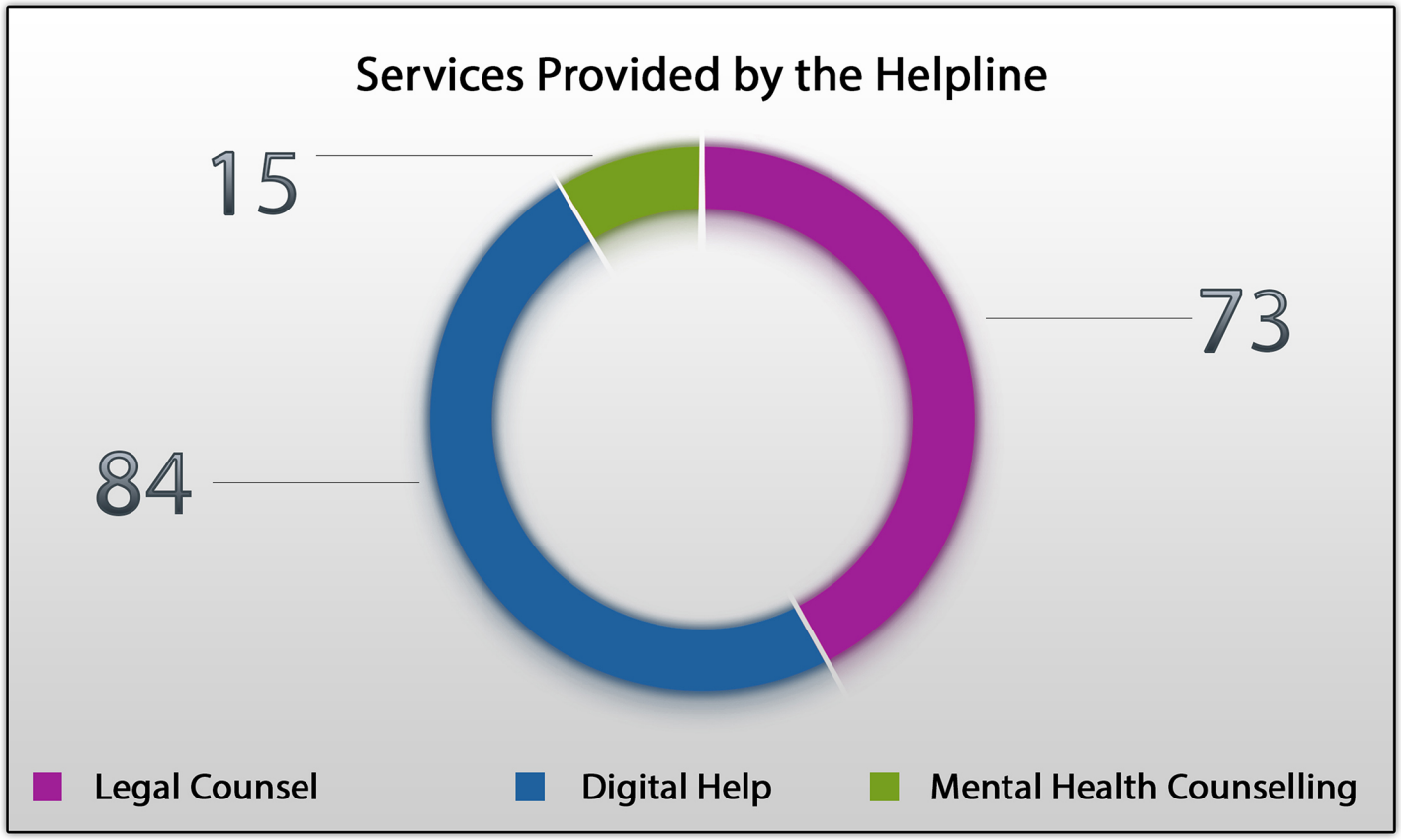


Figure 18: These statics are based on 6 months data collected from January till May 2018.

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:

It has come to light that the Rules u/s 51 of PECA have been drafted by the Ministry of Information Technology, two years after the passage of the law. These Rules have not been made public The Rules should expand the rights available to citizens and guarantee protections against intrusion in their digital spaces rather than further curtailing them.

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.

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. The FIA recently stipulated in a Senate hearing that it only has 10 cyber crime experts at its disposal. It has emerged that substantial amount of money has been allocated to the FIA for expansion into 10 additional cities, however there has been no official notification in part of the FIA regarding this expansion. 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. This is further exasperated 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. 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. 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.

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. 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.

---

13 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/.
14 "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/.
15 Zulqernain Tahir, "Rs2bn to be allocated for 10 cybercrime police stations," Dawn, October 4, 2016, https://www.dawn.com/news/1287879.

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, Cases marked as urgent should be expedited and dealt with on a priority basis.

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.These SOPs should be compliant with best practices regarding data protection, translated into regional languages and displayed clearly in all offices of the NR3C.

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.

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 cyber crime 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 cyber crime is processed at the local level.

12. 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.

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 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. It is also recommended that women's rights organizations be included and allowed to assist in developing these trainings.

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.

15. 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.

16. 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.

17. 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.

18. 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.

DigitalRightsFoundation

"KNOW YOUR RIGHTS"

www.digitalrightsfoundation.pk

/DigitalRightsFoundation

@DigitalRightsPK

/DigitalRightsFoundation