Recommendations of the Consultation on "Ways and Means to safeguard women from Cyber Crimes in India" organized by National Commission for women on 23rd July, 2014 at India Habitat Centre New Delhi

1. Recommendations to meet Legal challenges

i. Policies and stricter laws should be made to discourage hacking activities among the youth and discourage victims from approaching hackers for removing offensive contents from the internet, mobile apps etc.

ii. A woman centric information technology law must be drafted defining types of cyber crimes targeting women.

Sh. Alok Mittal, Commissioner of Police, Gurgaon addressed the delegates in the session on "Finalization of Recommendations for Policy Initiatives"

iii. Existing provisions of Information Technology Act and IPC must be reframed and a constructive law should be made. Provisions from Indian Telegraph Act, 1885 must be included in the new law.

iv. IT Act, 2000(as amended in 2008) is not women sensitive Act. It needs to be reviewed to introduce more innovative approaches in law.
v. The offences targeting online crimes against women must be made non-bailable and cognizant offences. The punishment terms must also be enhanced from simple imprisonment terms for 6 months/1 year, to minimum 3 years to maximum 5 years, or 7 years or more (in cases of grave offences).
vi. Uniform identification numbers may be created for use to create accounts in the social media.
vii. "Right to access the net", "right to be forgotten" policies must be incorporated and such rights must be given the status of fundamental rights.
viii. National commission for women should propose policies to include the issues of cyber crimes (especially crimes targeting women) in bilateral treaties. This would help in resolving cross-jurisdictional cases of cyber crimes targeting women.
ix. National commission for women should propose to the government for framing stricter guidelines for intermediaries to pull down any content offensive to women.
x. As trans - Jurisdictional issues are involved in most of the cyber crimes, there is a need to develop a trans jurisdictional mechanism by signing bilateral treaties.
xi. Under Section 357 A of CrPC, compensation is given to victims of crimes, who have suffered loss or injury as a result of the crime and who require rehabilitation. Compensation to victims of cyber crimes on similar lines may also be considered as consequences of female victims of cyber crimes are equally devastating.

Recommendations to meet socio-psychological challenges

i. More awareness programmes should be organized in schools and colleges in order to enable children and youth to learn about the dangerous consequences of misuse of information communication technology, existing and newly evolving varieties of cyber crimes targeting women and the general reasons for the growth of the issue, socio-legal ethics regarding photography in the public places (especially photography of women), to inculcate safe habits in the cyber space and to make them aware of legal rights and duties towards respecting right to privacy, right to life, liberty and child rights against abuses**.**

Smt. Shamina Shafiq, Member, NCW and chair of the session on "Finalization of Recommendations for Policy Initiatives" introduced the concept of the session

ii. Awareness camps must also be held for adults including teachers and parents regarding the duties to monitor children's behaviour in the internet, monitor the use of digital devices by young children, teach the children and matured teenagers about safety norms in the cyber space and encouraging them to report cyber crimes against women to parents, teachers and law and justice machinery.

iii. Government / Organizations must be encouraged to develop positive policies especially at workplaces to help women to come out of the 'feeling of shame' and report crimes to proper authorities.

2. **Recommendations to meet Technical/Implementation challenges**

i. Hotlines numbers such as 1098, 1091, 100 should be made functional to receive complaints and these numbers should be exhibited in all schools, colleges, universities, corporate organisations etc.
ii. Policies on compulsory training of all the police officers for dealing with cases on information technology, for creation of cyber crime cells in all police stations and for deputing more women officers and women judges to deal with cases of cyber crimes against women must be implemented.
iii. Cyber forensic labs in each district police head quarters should be set up. Over all, proactive policing for dealing with cases of cyber crimes against women is highly recommended.
iv. Laws (such as Ss.292 and 294 IPC) and policies for restricting illegal and unauthorized selling of digital devices and porn contents by local shops should be strictly implemented.
v. *Mahila courts* which are dealing with cases concerning women such as dowry harassment or custody cases for children may be given the power to deal with cases of cyber crimes against women.
vi. Websites / organizations working to help victims of cyber crimes must collaborate with National Commission for Women for a common goal of curbing the issue.
vii. Women friendly mobile apps with a special chip or provision that can detect misuse of such apps in the name of helping women in distress may be

developed.

viii. Law enforcement agencies should be strengthened by opening more Cyber Cells, dedicated helpline numbers and imparting of proper legal and technical training to law enforcement agencies like police and judiciary to combat cyber crimes at every level.

ix. Issue of cyber crimes also needs to be taken up at workplaces. IT policies of the companies should be transparent and hidden cameras installed at workplaces in personal space of employees to keep watch on productivity of workers should be avoided.

x. Police and policing is not complete solution. Role of Social Media and self restraint are also important.

xi. Proper cooperation between victims, police, judiciary, social media, service providers and various stakeholders is required to deal with cyber crimes.