

BEFORE SH. RAJESH AGGARWAL, ADJUDICATING OFFICER,
INFORMATION TECHNOLOGY ACT 2000, GOVERNMENT OF MAHARASHTRA,
AT MANTRALAYA, MUMBAI – 400032

Complaint No. 2 of 2010

IN THE MATTER OF

1. Sh. Vinod Kaushik
2. Sh. Neeraj Kaushik

..... **Complainants**
Through Mrs. S.R. Padhy, Advocate

Versus

1. Ms. Madhvika Joshi
2. Sh. Atul Tripathy
3. Ms. Monika Agnihotri
4. Cognizant Technology Solutions Pvt. Ltd.

..... **Respondents**
Through Mrs. Vaishali Bhagwat,
Advocate for R 1-3,
and Sh. Amit P. Gagh, Advocate for R-4

ORDER

This case is primarily against Respondent No. 1 by her Father-in-law and Husband (Complainants) for accessing their Gmail accounts and using some emails and chat session print outs as evidence in the Dowry Harassment case lodged by her against them. This case was originally heard by my predecessor Dr. Ajay Bhushan Pandey, and he passed order dismissing the Application on 9th August 2010. Against this, the Complainant Sh. Vinod Kaushik (along with

Sh. Neeraj Kaushik) appealed to Cyber Appellate Tribunal, where Hon'ble Justice Sh. Rajesh Tandon, Chairperson of the Tribunal passed order on 29th June 2011, asking the Adjudicating Officer to decide the matter afresh in accordance with the observations made in the order. Mainly these observations were regarding proper impleadment by Appellant No. 2 (Sh. Neeraj Kaushik) before Adjudicating Officer, and second on whether proceedings against Respondent No. 4 (Cognizant Technology Solutions Pvt Ltd, Pune) had been dropped by the Adjudicating Officer.

Without repeating the full history of the case, which is available in the two orders mentioned above (by Adjudicating officer and Cyber Appellate Tribunal), I would focus on the substantive issues. In hearings before me, Complainant No. 1 (Sh. Vinod Kaushik) and Respondent No. 1 (Ms. Madhika Joshi) appeared personally, and through their learned advocates. Respondent numbers 2, 3 were represented by same advocate as for Respondent number 1, while Respondent No. 4 was represented by their advocate. Complainant No. 1 (Sh. Vinod Kaushik) maintained that his son Sh. Neeraj Kaushik (Complainant No. 2) was being represented by him, and produced a document signed by Sh. Neeraj Kaushik authorising it. However, learned Advocate for Respondent No. 1 took objection in first hearing that while the document mentioned that signature of Sh. Vinod Kaushik is confirmed "as below", the document actually bore no signature of Sh. Vinod Kaushik. During next hearing(s), Sh. Vinod Kaushik brought the same document with his signature appended. Learned Advocate for Respondent No. 1 pointed out that this did not bear fresh "confirmation" by Sh. Neeraj Kaushik, and did not bear new date, but she said she will not press this technical point further.

I find that in the original case before the Adjudicating officer, the Vakalatnama has signatures of both Sh. Vinod Kaushik and Sh. Neeraj Kaushik, though the Application is filed by Sh. Vinod Kaushik only. In the Appeal before the Tribunal, both have filed the Appeal, and in the renewed hearings before me, Sh. Neeraj Kaushik has given "authority" to Sh. Vinod Kaushik as stated in above paragraphs. Hence I conclude that both should be considered as Complainants, without dwelling too much on the technicalities.

With this point concluded, I would like to now focus on whether any case is made against Respondents 2 to 4. No new substantive material or

arguments were made by Complainant or Respondents 1 to 3, except the respondents repeating that Complainants have no proof against the two colleagues of Ms. Madhika Joshi, and that Complainants have dragged them in as they appear as witnesses in Dowry case. In statements before the Police, Respondent No. 1 has clearly said that she looked at emails and chat sessions on her own, and her colleagues were not involved. I also find absolutely not a shred of evidence given by Complainants against Respondents 2 and 3. Hence I conclude that Respondents 2 and 3 have committed no contravention of IT Act, and no case is made out against them.

Regarding Respondent No. 4 (Cognizant company), I find no orders on file dropping them from the case. Hence they are involved as Respondent No. 4 in this case. The Complainants' advocate said that Companies are supposed to ensure that employees do not "misuse internet" or company resources. The learned advocate appearing on behalf of the Company stated that though Cognizant discourages employees from using the internet for personal use, it does not block internet access to employees and does not monitor what employees are doing. I find that this is quite fair and the IT Act does not force Employers to act like "Big Brother", to install key loggers or similar such methods. It is for Companies to state their policy clearly to employees and any violation need to be acted upon as per their HR policies, and not under IT Act. The IT Act and other laws expect Employers, and IT intermediaries to cooperate with Police and Courts in case any evidence or logs are demanded from them. In present case, I see no evidence of any non-cooperation, and see no wrongdoing on behalf of the Company, and conclude that no case is made out against Respondent No. 4.

The substantive case is between the two Complainants and Respondent No. 1. During arguments, both parties have extensively quoted from some international cases as reported on various websites on the internet. I would dwell on the major points one by one.

"Hacking" is generally understood in English language to mean that the hacker tweaks hardware/software to get access to somebody else's computer, systems, website etc, to gather/use credit card data, steal military or business secrets, even change exam results, to cause national embarrassment by defacing websites, or to cause random mayhem, etc. If password is weak, and

is easily "cracked" by a few intelligent guesses, it still is hacking. If password is carelessly left in a notebook nearby, it still is unauthorised access. This is where things start taking interesting shape. If someone has innocently or foolishly put his/her password on a yellow slip glued to their desktop, or written it on the wall nearby, does it give anyone else authority to log into the system and say it is not hacking because "the idiot should have kept his/her password safely"? If someone leaves his door key under the mat of the front door, can the thief say that the house owner was asking for it?

Now, between the family members, especially between spouses, sharing of computers, reading each other's Facebook pages or emails, picking up each other's mobile phones and reading SMSes, or even opening letters arriving in envelopes is pretty common, especially in Indian context. Does a mother have a "right" to search through the kid's bag when he comes home, trying to keep the kid away from "bad habits"? Does a husband have a "right" to open the letters arriving in wife's name and read them? Does the wife have a similar right? Or does this "right" become invasion of privacy when the other spouse/person feels irritated at this? Does it become "unauthorised access" if the couple lose trust in each other and/or break up and start living separately, without a formal divorce?

As families are becoming Nuclear rather than big joint families, and especially in urban areas, family members are becoming more conscious of "personal space" and need to respect the boundaries of privacy. One suspicious spouse (or even an overzealous mother) seeing the others emails, SMS messages, last dialled numbers on mobile phone, websites visited by him/her can lead to breakdown of relations. In cases of divorce, many such issues do come up in courts, especially in the Western countries. Suspicious husbands and wives try to look for evidence - "lipstick on the collar", long hair on shirt, smell of new perfume, SMS messages between ex-lovers, letters from ex-lovers or current lovers in the cupboard, emails and chat sessions etc. Does this amount to invasion of privacy and unauthorised access? Is such "evidence" admissible in court? Even if admissible, does it exonerate the party which collected evidence through questionable means? Or does this "evidence collection activity" become a "crime" if other party is declared innocent by court, and does not become a crime, if other party is convicted? In some cases

in Western countries, the spouses looking into the other's computers have been let off with a warning, in some cases fined, and in some cases let off completely as "this is an internal family matter" not fit to waste court's time and taxpayer's money.

In the present case, there is dispute over the time period (duration) for which the emails of Complainants' were accessed by the Respondent No. 1. However, she clearly admits to opening the Gmail accounts of both Complainants a multiple number of times, after the couple had started living separately, and she had filed Dowry case against the Husband and the in-laws. Her defence is two-fold: one, she did not "hack" as the husband had willingly shared the passwords earlier, and second, she did this as "self defence", to collect evidence against them.

As far as the question of knowledge of password is concerned, it is quite clear from the papers produced by Respondent No. 1 that Complainant No. 2 (husband) had shared passwords with her and also mentioned to her that password of Complainant No. 1 was same as that of Complainant No. 2. The records produced by Complainants do not prove that they changed the passwords. Hence, a reasonable conclusion is that Respondent knew the passwords, and she took Complainants by surprise by accessing their Gmail accounts, looking at dozens if not hundreds of emails and chat sessions, and forwarding/printing those emails and chat sessions which she thought would help her in the Dowry case. Respondent heavily argues that there is a "bond of trust" between husband and wife and hence she had "right" to access the emails. As the emails have been accessed after this "bond of trust" was broken, and dowry case was lodged, and husband arrested, I find no merit in this argument. Section 43 of IT Act clearly applies, regarding unauthorised access. The Respondent has not only accessed the email account of her husband, but also of her father-in-law, and has taken print outs of chat sessions between the husband and his friends, including those with wife of his friend, and also of her father-in-law's chat sessions with his relatives and friends. Thus, she has violated the privacy of not only the Complainants, but also of their friends and relatives, who had by no stretch of imagination, authorised her to look into these private chat sessions. Even in family or company premises, if someone has forgotten to log out, and another person

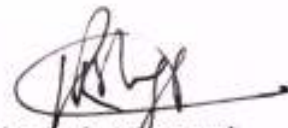
comes across the open emails when he/she tries to log into their own Gmail (or other email or Facebook or Skype etc.) account, the normal expectation is that the new person will immediately log out and not snoop into other emails or chat sessions. Thus it makes a vast difference whether you glance at an open email, or log into a closed email box using a password and look at the emails. This is similar to the difference between looking at an open letter lying around; versus opening a sealed envelope which clearly is meant for somebody else. Hence regardless of the fact whether the Respondent No. 1 knew the passwords, or made intelligent guesses, or used some software to crack the passwords, it is clear that she unauthorisedly accessed the emails and chat sessions, and violated the provisions of IT Act. The Respondent had no authority to open these Gmail accounts, especially of her father-in-law and downloading his chat sessions. If she had any suspicion that material evidence of wrongdoing could be found, she should have approached the Police regarding this, and let the Investigative agencies take action as per law.

Now, the next question is regarding the damages asked by the Complainants. Here the Respondent's defence is that she did not use the material in any other way than giving it to Police and Courts, and hence she is not liable for any damages based on action taken by the Police/Courts. Her learned advocate mentioned during argument that on the other hand, Complainants went to media portraying her as a hacker, defaming her. The Complainants have drawn attention to "repetitive nature of default" under Section 47 of IT Act, and mention about loss caused by missing career growth opportunities, loss of business and loss of reputation. After carefully going through all the Records available before me and arguments made by various parties, my conclusion is that the principles of Natural Justice and balance of convenience lie mainly in favour of Respondent, as she used the "evidence" so collected only to give it to Police and the Court, and did not make it widely public. If the Police action or Court action has resulted in any kind of loss to the Complainants, the Respondent cannot be blamed. It is also relevant to note that the evidence is being used in a Dowry case, filed within first few months of marriage. Hence, despite the fact that unauthorised access is proved, the case for heavy damages is not made out.

As far as the question of admissibility of evidence collected by questionable means in the dowry case is concerned, it is for the Hon'ble courts to decide the use of such evidence on case to case basis, as the context and circumstances of each case are highly different.

Under IT Act, the Adjudicating officer has to decide on basic two questions – whether IT Act was violated and if yes, then what punishment is due. Based on above circumstances and arguments, I conclude as following:

1. Respondent No. 1 has violated Section 43 of IT Act, and made unauthorised access to Gmail accounts of her husband and her father-in-law, and unauthorisedly downloaded/forwarded/printed their emails and chat sessions with others, thus committing Identity Theft by using the password belonging to others dishonestly, and violating the privacy of not only the Complainants, but also of others with whom these chat sessions were conducted.
2. Given the fact that she gave the evidence only to Police and the Court, in the Dowry case lodged by her against her husband and in-laws, and did not make it widely public, I do not hold her liable for damages. Under section 66-C, there is provision of fine for Identity Theft, for dishonest use of password of any other person. I order that she pay a token fine of Rupees One Hundred to the State Treasury.
3. No case is made out against Respondents 2 to 4.
4. No order as to the costs by the Parties.



(Rajesh Aggarwal,

Secretary (Information Technology),
Government of Maharashtra,
Mantralaya Annexe, Mumbai-32