CENTRAL INFORMATION COMMISSION
Club Building (Near Post Office)
Old JNU Campus, New Delhi - 110067
Tel: +91-11-26101592

File No. CIC/BS/A/2012/001725
16 December 2015

Relevant Facts emerging from the Appeal:

Appellant	:	Mr. Maniram Sharma Nakul Niwas, Behind Roadways Depot, Sardarshahar, District: Churu- 331403, Rajasthan
Respondent	:	CPIO & Scientist "D" **M/o Communication & IT** **National Informatics Centre** **RTI Division** A-Block, CGO Complex, Lodhi Road, New Delhi - 110003
RTI application filed on	:	24/05/2012
PIO replied on	:	28/06/2012
First appeal filed on	:	04/07/2012
First Appellate Authority order	:	23/08/2012
Second Appeal received on	:	23/10/2012

Information sought:
Please arrange to provide me the following information:-

1-Copy (in a CD) of all email addresses details of Govt/Public authorities/ organizations maintained by NIC with up-to-date amendments therein.

Grounds for the Second Appeal:
The CPIO has not given the satisfactory information.

I. Relevant Facts emerging during Hearing:
The following were present

Appellant: Mr. Maniram Sharma through TC M 09460605417
Respondent: Shri Ambreesh Kumar FAA & Mr. Swarup Dutta CPIO.

The CPIO stated that the information cannot be provided due to security reasons and can be misused. The Appellant argued that the e-mail addresses/ids of Government and public sector organizations are freely available on their individual websites and in fact it is Government policy to encourage use of e-mail for correspondence to avoid unnecessary paper work. He further stated that he has mentioned in his submissions to the FAA, that in case the Respondent feels there are certain sensitive information, the same may be severed as per Section 10 of the RTI Act but the disclosable information cannot be denied to him. He added that since the Respondents have not provided information within the mandated time, the same should now be provided free of cost as per Section 7(6) of the RTI Act. The CPIO stated that an opportunity may be given to him to make written submissions in the matter, as he strongly feels that the information is exempt from disclosure.

Interim Decision notice:

As requested by the CPIO it is decided to grant adjournment and invite written submissions from him demonstrating in detail his stand on the issue at hand, so that full facts are brought on record. Accordingly, the CPIO should furnish his submission to the Commission (endorsing a copy to Appellant) by 15/11/2013.

The hearing is adjourned for **16/12/2013 at 04:00 p.m.**

II. Relevant Facts emerging during Hearing:
The following were present

Appellant: Mr. Mr. R K Jain Appellant's representative
Respondent: Mr. Swarup Dutta CPIO

The Appellant's representative after going through the written submissions of the CPIO argued that the domain address *"nic.in"* is owned by the Respondent and during the last hearing the Appellant had acceded to deletion of sensitive information viz. the information relating to security organizations as listed in Section 24 of the RTI Act. He further argued that the name and address is not personal information and therefore no ownership can be claimed for it. He pointed out that large number of mails sent by him to the domain address as available on the website of public authorities bounce back and hence, it is in public interest to display the up-to-date information on the "nic" website. The CPIO pleaded that one more opportunity may be given to him to make written submission in the matter and added that he will also bring the deemed CPIO for the next hearing.

Interim Decision Notice:

As requested by the CPIO it is decided to grant one final adjournment in the matter. Accordingly, the CPIO should furnish his written submission to the Commission (endorsing a copy to Appellant/his representative) by 10/1/2014.

The hearing is adjourned for **20/01/2014 at 04:00 p.m.**

III. Relevant Facts emerging during Hearing: (20/01/2014)

The following were present

Appellant: Mr. Mr. R K Jain Appellant's representative

Respondent: Mr. Swarup Dutta CPIO & Mr. CLM Reddy

The CPIO stated that he has two key arguments for not releasing the information:

(i) The release of all e-mail addresses can be a security threat and can choke the Government network and block access to the NIC servers.

(ii) The information relates to third parties including sensitive organizations and they do not have the resources to carry out the exercise as outlined under Section 11 of the RTI Act for seeking individual consent on the disclosure of information.

The Appellant's representative stated that the Respondents should give their written submissions in the matter to enable him to submit his rebuttal, if necessary.

Interim Decision notice:

It is decided to adjourn the matter to enable the CPIO to give his written submissions to the Commission by 20/02/2014. A copy of the submissions should be provided to the Appellant for his rebuttal, if any.

It was considered expedient to place the case before a larger bench to hear and adjudicate on the issues involved in the matter. Accordingly a Full Bench comprising Hon'ble Information Commissioners Mr. Basant Seth, Mr. Yashovardhan Azad and Mr. Sridhar Acharyulu was constituted and notices issued, intimating the adjournment of the matter, to be heard on **11/03/2014 at 3:00pm**.

IV. Relevant Facts emerging during Hearing: (11/03/2014)

The following were present

Appellant: None for Appellant

Respondent: Mr. Swarup Dutta, CPIO; Mr. CLM Reddy, AA & DDG and Ms. Seema Khanna, Technical Director

The CPIO reiterated his arguments denying disclosure of information citing the key reasons as follows:

(i) The information sought is neither generated nor held by the public authority since their role is limited to providing the domain to the concerned organization. Creation/generation or maintenance of any data/content therein does not fall within the purview of their service agreement(s).

(ii) The release of all e-mail addresses at one place is likely to render the system vulnerable to security threat. It can also lead to choking of the Government network and blocking of access to the NIC servers by random and enormous amount of spam mails.

(iii) The information relates to third parties including sensitive organizations and they do not have the resources to carry out the exercise as outlined under Section 11 of the RTI Act for seeking individual consent to the disclosure of information.

Upon being probed by the Bench, the representative(s) of the Public Authority narrated that providing such huge data at one place in one hand could cause security threat since the same can be misused and abused very easily at the click of a button to jeopardize entire systems linked by internet. Most importantly, the NIC submitted that they are neither the owner nor the custodian of the information sought. They explained that the role of NIC as a service provider consists of providing the domain to each organization. It is the respective Admin console which creates the email addresses of the employees of the organization and decides the content of the website. Creation, activation or even deactivation or deletion of such email addresses in the event of prolonged non usage, is controlled entirely by the respective organization. NIC has no access to the data of the organization.

The Bench at this stage sought a detailed and specific submission from the Public authority to elucidate its exact job profile in respect of the service/s provided to the various Government authorities. The Respondent sought time to place the same before the Bench. To a query by the Bench as to whether the information sought is already in public domain, the Respondent submitted that they have no idea about the same.

The Bench also enquired about the opinion of CERT – Computer Emergency Response Team and was informed by the Respondents that the same had been sought by the NIC and response was awaited. The Commission emphasized that the aspect of “security threat” need to be established better by the Respondents if they seek exemption from disclosure on such ground.

Interim Decision notice:

In view of the pertinent questions that arose during the course of the hearing, the Commission is of the considered opinion that more specific submissions on the aforementioned queries need to be submitted by the Respondent. The CPIO sought four weeks time to submit the same. Accordingly, it is decided to adjourn the matter to enable the CPIO to give his written submissions to the Commission within a month. A copy of the submissions should be provided to the Appellant for his rebuttal, if any.

The hearing is adjourned to 22.04.2014 **at 03:30 p.m.**

V. Relevant Facts emerging during Hearing: (22/04/2014)

The following were present

Appellant: Mr. R K Jain was present on behalf of the Appellant

Respondent: Mr. Swarup Dutta, CPIO; Mr. CLM Reddy, AA & DDG and Ms. Seema Khanna, Technical Director

At the very outset, the representative for the Appellant, Mr. Jain submitted some additional documents before the Bench which included a judgment of the Madras High Court and some information from the website of ICERT. He opened his arguments with the submission that he waived off any claim to information relating to any Government organisation exempt from the purview of RTI Act under Section 24 of the Act. Mr. Jain further contended that the arguments of the Respondent/s, in stating that they are not the holders of the information is contradictory to their contention apprehending threat to national security. While admitting that email addresses of Govt functionaries though available on their respective websites, the Appellant's main emphasis was on the "up-to-date" record of all email addresses details of Govt/Public authorities/organizations maintained by NIC with recent amendments, in a CD. It was his case that a number of email addresses which exist on the websites are non-functional and hence any communication addressed to such addresses normally bounces back. Hence, in order to facilitate better reach of the benefits of e-governance to all the citizens, in his view it was imperative that an updated record revealing all email addresses details of Govt/Public authorities/organizations maintained by NIC be made available.

While countering the arguments of the Respondent, the Appellant's representative stated that Applicant under RTI Act is not under any mandate to cite any reason for seeking the information. He further argued that information cannot be denied merely on the apprehension that the same could be misused since information could be denied only when the same was covered by the provisions of the Section 8 or 9 of the RTI Act and not otherwise.

The CPIO reiterated his arguments denying disclosure of information on the grounds as stated below:

(i) The Respondent is neither the owner nor the holder of the information sought and their part in providing the service is limited to providing the domain to the concerned organization. The creation/generation or maintenance of any data/content therein does not fall within the purview of their service agreement(s) with the respective Govt/Public authorities/organisations.

(ii) The release of all e-mail addresses of the Public authorities in a CD could lead to humungous amount of unwanted internet communication sent from fake IP address/es choking the Government network and blocking access of the NIC servers thereby posing security threat to the e-governance systems set up nation-wide.

(iii) The information relates to third parties including sensitive organizations and NIC does not have the resources to carry out the exercise as outlined under Section 11 of the RTI Act for seeking their individual consent to the disclosure of information.

At this juncture, the Bench probed that in case there is such an imminent danger of such magnitude to national security, it is important that the Commission is apprised of the same by the Respondent, based on past instances and experiences where abuse of cyber access at this level have crippled the entire Government/private machinery. The Commission directed that the Respondent must clearly establish the scale and enormity of the likely damage as have been repeatedly contended by them. Secondly, the Commission wanted to know whether providing a record of some key email addresses related to important departments closely connected to the PDS systems, generally required by any citizen, would suffice the requirement of the Appellant. The Commission seeks to know whether any mechanism can be devised in order to collate such data of the officials in essential public service related roles and can be made readily available to the citizens at large.

The parties sought time to respond to the queries put forth by the Commission and make appropriate submissions.

Interim Decision notice:

In view of the queries and issues which still require clarification and corroborative facts, the Commission grants some more time and another opportunity to both Respondent and Appellant to place forth their respective contentions within four weeks' time. Accordingly, it is decided to adjourn the matter, while the parties are directed to exchange their submissions before the next date of hearing.

The hearing is adjourned to **27/06/2014 at 04:00 p.m.**

VI. Relevant Facts emerging during Hearing: (27/06/2014)

The following were present

Appellant: Mr. R K Jain was present on behalf of the Appellant
Respondent: Mr. Swarup Dutta, CPIO & DDG and Ms. Seema Khanna, Technical Director

The Appellant was represented by Mr. R K Jain who commenced his arguments citing the failure of the Respondents in replying to the Commission's specific query about "….past instances and experiences where abuse of cyber access at this level have crippled the entire Government/private machinery…".Thereafter the Appellant proceeded to make submissions/arguments on the following points:

1. He agreed at the very outset to forego all the information relating to organisations which are exempt under Section 24 and under Section 8 of the RTI Act or any information which could be termed sensitive from national perspective.
2. Next the Appellant stated that in keeping with the initiative of Citizen's Charter it is imperative that information of the email addresses be provided in line with the precedent set by the Government of Uttarakhand which published a 36 page list on its official website disclosing 1500 email addresses of prominent Government functionaries. He laid emphasis on the fact that despite such disclosure by one of the smaller State Governments (which has been last updated on 14/11/2013) neither attack nor threat, as apprehended by the Respondent, has been reported till date. The Appellant averred that rural development and overall development of the nation will get a boost by adhering to the Citizen's Charter and disclosure of the information (i.e. key official email addresses in this case), since the basic objective of the Citizens' Charter is also to empower the citizen in relation to public service delivery.
3. The Appellant argued that email address is nothing but a virtual address and disclosure of official email address thus falls within the ambit of disclosure as defined in Section 4(2) of the RTI Act. He has added that as a practice, each Government department/Ministry discloses such information on their website, then how disclosure of such information collectively can through one medium alone pose a threat? Without prejudice to his rights, the Appellant was even agreeable if all the relevant information (emails as he sought) was uploaded by the Respondents on their website, even if he does not get them in a diskette form.
4. The Appellant in his arguments touched upon the provision and applicability of Article 51A of the Constitution which enumerates the eleven Fundamental Duties as laid down by the Constitution of India.

Further rebutting the contentions raised by the Respondent, the Appellant stated as follows:

1. The apprehensions of misuse or abuse of information or even of "misuse for commercial purpose" are not valid grounds of exemption which can be entertained under the RTI Act.
2. In response to the Respondents' persistent averment that the information sought is "neither generated nor held by the NIC", the Appellant points out contradictory submissions of the Respondent claiming that "as a matter of policy NIC does not share the email repository with anyone". The argument about Terms and Conditions of Email application form binding upon NIC for prevention of disclosure of information has also been demolished by the Appellant stating that RTI Act being a statutory Act, provisions therein prevail over and above any such restrictive Contractual obligations.
3. The Respondents' contention (in the submissions dated 21.04.2014) that NIC does not have the resources to carry out the process under Section 11 is rebutted by the Appellant stating that applicability of Section 11 arises only when the information to be disclosed is treated as confidential by the Third party.

The Appellant made additional submissions stating:

i) It is necessary to implement methods and technology to be able to block mails which the Respondents apprehend can choke and cripple the Government network and block access to the NIC servers.

ii) In addition the Appellant also pointed out that apart from mechanisms like Firewalls and Filters, the CERT-In [Indian Computer Emergency Response Team] as an organisation caters to this precise and vital task of tackling and overcoming such threats or attacks on Government cyber space and/or machinery.

iii) The Appellant was agreeable even if the disclosure of information was by way of uploading of the information on the website of the Respondent instead of providing the same in a CD form, as sought in the RTI application.

iv) The Appellant has also submitted that even CERT in its submissions has expressed mere apprehensions and conjectures of various possibilities, without explaining the actual threat in a comprehensible form.

v) It is suggested and desired that infrastructure of Government machinery needs to be upgraded to meet the growing demands of time and for a comprehensive and wholesome development of the nation it is imperative to disseminate which secures access of citizens to their fundamental rights of everyday necessity. Devising appropriate mechanism to combat attacks/threats is recommended over withholding of information for fear of misuse.

The Respondents in their submissions mostly reiterated their previous arguments. In a gist their contentions were as follows:

1. NIC does not own nor generate data and is contractually debarred from disclosure thereof;
2. To the specific query of the Commission about the "….past instances and experiences where abuse of cyber access at this level have crippled the entire Government/private machinery…", the Respondent stated that instances of such attacks cannot be divulged for public consumption and NIC is not allowed to share information. Threats are handled on everyday basis. The Respondents submitted that since the data is huge, the threat shall be unknown and the NIC is apprehensive, clueless and uncertain about the kind of measures needed to handle the imminent danger to national security, while potent.

With a view to gain better perspective on the repeated plea of the Respondent that disclosure of information as sought by the Appellant was likely to cause imminent danger to national security in this case, the Commission found it appropriate to seek the views of an independent expert in cyber security and cyber laws in order to gauge the technical aspect of the matter. Accordingly notice was sent to a cyber expert viz. Mr. U. Rama Mohan, Additional SP, CID, Cyber Crimes, Hyderabad to join in a hearing of this case on 12/12/2014 with copies to other relevant parties. The hearing was held specifically to obtain the views of the independent expert on the disclosure of information as sought by the Appellants.

VII. Relevant Facts emerging during Hearing: (12/12/2014)

The following were present

Appellant: Mr. R K Jain was present on behalf of the Appellant

Respondent: Mr. Swarup Dutta, CPIO & DDG and Ms. Seema Khanna, Technical Director,
Mr. U. Rama Mohan, Additional SP, CID, Cyber Crimes, Hyderabad [through video conferencing]

The Additional SP, CID, Cyber Crimes Sh. Rama Mohan participated in the hearing through video conference and opined that:

1. Providing all email IDs issued by NIC, on NIC portal is to be discouraged for threat of spamming from unknown enemy from anywhere. He further added that spam filters are meant only for certain keywords and do not provide full fledged security solution.
2. Email IDs of persons not connected with direct public service and those connected with public dealings should be segregated in order to avoid confusion to the applicant.
3. NIC simply creates and issues the email id-s for various Government departments, but as per the IT Act, the user is the owner of the email id who reports any hacking of the account and not the issuing authority.
4. NIC would require permission before providing email id-s so as not to attract provision of the Section 72 of the IT Act.
5. A recent act of defacing of 22 websites by criminals, maintained by NIC indicate vulnerability and possibility of unauthorized access despite quality security measures. In the event of voluntary publication of entire list of email IDs, commissioning of such offences will become relatively easy.
6. Mail ID spoofing of senior officers, circulating to junior officers will become very easy for criminals as will be attacking individual computers from remote servers with programs like Cryptolockers.
7. Since issuance of the email IDs is a dynamic process, publishing the information relating to the officers directly connected to public may be very laborious and tedious task.
8. Individual mail IDs configured in smart phones and tablets of the officers, will automatically reveal physical location of the officers, thereby compromising their personal safety and security.
9. Publishing such information may be detrimental to security measures.

Pursuant to this, the Commission received written submissions dated 19/01/2015 from the Appellant objecting to the inclusion of Sh. U. Rama Mohan, Addl. SP, Cyber Crime in the hearing on 12/12/2014 and seeking his opinion about the feasibility of disseminating the information. The Appellant while seeking a hearing to voice his objections before the Full Bench has contended that the opinion sought from Sh. U. Rama Mohan is inadmissible in this case since neither he was

a party to the proceedings nor did the Cyber expert seek any permission from the Commission to intervene in this matter and even none of the parties to the hearings viz. the Appellant/Respondent requested for the expert to be examined, hence the Appellant contends that Sh. Rama Mohan has no *locus standi* to be examined like a witness/expert in the matter. The Appellant has further objected that arguments in the matter were extensively heard and the matter closed for passing of order on 27/06/2014, hence legally the case could not have been reopened *suo motu* to include the testimony of an expert, whom the Appellant chooses to consider a planted tutored witness in the matter. Accordingly, the Appellant has categorically argued that no credence can be attached to his evidence since the status of Sh. U. Rama Mohan could not be determined from the records of the CIC and also because according to the Appellant Sh. Rama Mohan being a serving officer on Preventive and Enforcement duties in Andhra Pradesh Police cannot be considered an independent witness because of apparent conflict of interest. Thus the Appellant has strongly opposed the admissibility of the views/opinions/evidence of Sh. U. Rama Mohan. While challenging the superiority of expertise and knowledge of Sh. Rama Mohan over the Respondent, the Appellant contends that introduction of a third party who is unconcerned with the matter at a stage when the hearing in the matter was already closed is highly improper, irregular and illegal.

VIII. Relevant Facts emerging during Hearing: (21/04/2015)

The following were present

Appellant: Mr. R K Jain was present on behalf of the Appellant

Respondent: Mr. Swarup Dutta, CPIO & DDG

The Appellant's arguments focused only on his objections about the evidence of the Cyber expert Mr. U Rama Mohan and was in line with his written submissions dated 19/01/2015, as detailed in the paragraph above. The Appellant concluded his submissions stating that clarification if any required in the matter can well be supplied by either of the parties viz. himself or the Respondent, which is a specialized body handling all cyber issues for Government departments pan-India. The Respondents chose to reiterate their previous submissions about non supply of the information, as has been extensively dealt with in the preceding paragraphs.

DECISION

1. The Commission has heard detailed arguments of the parties and perused the documents submitted by them. The contentions of both the sides at a glance are as below:

No	Contention of CPIO	Appellant's claim for information
1.	Release of email addresses is likely to be a security threat and can choke the Government's net work.	No specific past incident is shown.
2.	Release of all emails in CD could lead to humungous amount of unwanted communication such as Denial of Services attack. Threat of spamming from unknown enemy from anywhere. Smart cell phone holders can find the physical location of email id owners.	Mere apprehension cannot form basis of denial. The NIC or CERT-IN should develop the mechanism to prevent the security threats and choking in attacks.
3.	Emails are already available on official websites of the respective Ministries	That makes it imperative to disclose them.
4.	NIC neither generated nor holds the information sought. Their service is limited to providing the domain. NIC simply creates and issues email ids to various government departments, which as per IT Act are the real owners of those email ids. Section 72 of IT Act requires the permission of concerned departments.	NIC agreed that it has generated. Even if it does not own, if it holds that information that is enough under RTI Act to provide information subject to other provisions of Act.
5.	Information relates to third parties including some sensitive organizations. It does not have resources to implement the process required under Section 11 RTI Act.	The information that is to be disclosed under Section 4 is not third party information. Lack of resources is no defence to deny the information

2. From the hearings accounted above, it further emerges that the appellant waived off the pursuit of certain information and gave suggestions, which are as follows:

(i) Information about organizations exempt from RTI Act under Section 24.
(ii) NIC can use technology to prevent or block access of those who try to choke or cripple the Government network

(iii) Need not give email ids in the form of CD as sought in RTI application, it is enough if placed on website, after removing the information that is exempted under Section 8(1) (a) on the ground of security.

3. Mr Sarabjit Roy, National Convenor, India Against Corruption was present in one of the hearings and made the following significant submissions:

(i) "*nic.in*" is not the official domain of Government of India, hence all email IDs with suffix *@nic.in* need not be official.

(ii) Only those reserved domains like *gov.in, presidentofindia.in, primeminister.in, mea.in, mod.in, supremecourtofindia.in, eci.gov.in, goi.in, cabsec.in, goidirectory.in* etc totalling at most 20-25 domains.

(iii) He expressed apprehension that blanket disclosure would invite security risks.

(iv) Users of *nic.in* IDs have right to privacy and they need not be disclosed especially to a commercial publisher.

Mr. Roy concluded his submissions stating that at best the departmental web-coordinators nominated to interact with NIC may be directed to pursue their Section 4 mandates by updating their departmental disclosable email IDs to some centralized official server like *goidirectory.in* which is especially created for this purpose and the role of NIC may be that of technology facilitator.

4. Before proceeding to decide the case on merits, it is imperative that the arguments addressed by the Appellant on the last date of hearing i.e. 21/04/2015 regarding inadmissibility of the evidence of the Cyber expert Mr. U Rama Mohan and the alleged illegality therein, are dealt with. First of all, the Bench finds it relevant to clarify the fact, that contrary to the Appellant's submission, the opinion sought from the Cyber Expert was not a sudden proceeding but the relevant parties representing the case duly notified by the same notice dated 27/11/2014 as the Expert himself and accordingly, all the relevant parties including the Appellant were present during the hearing held on 12/12/2014. No objection was tendered by the Appellant during the said hearing dated 12/12/2014. Secondly, the recent hearing dated 21/04/2015 was in fact fixed because the Appellant had filed an application seeking a hearing, and a fair hearing has been rendered to him, in keeping with the tenets of natural justice. Thirdly, the expert opinion in this

case was sought from the concerned official placing reliance on the office held by him by virtue of his expertise and knowledge as deemed fit by the Bench, in the capacity of an "Expert" and not as a "Witness" as argued by the Appellant. The objections of the Appellant opposing the expert opinion on various counts are not tenable in law. The practice of various Courts seeking expert assistance in arriving at decisions involving complex or technical issues is not a rarity nor is the practice of appointment of an *amicus curae* unheard of or illegal per se. To elucidate this fact it is pertinent to mention the Delhi High Court's decision dated 06/12/2012 in WP (C) No. 8916/2011 titled **AIIMS vs. Prakash Singh** wherein it has been held as follows

> *…The Division Bench has also observed that they would be loathe to interfere in areas where academicians, being experts, have expressed a view, to the effect that, disclosure of question papers and keys would compromise the selection process….*

5. In fact this position has been discussed more emphatically and the role of experts accorded supremacy in the recent decision dated 13/03/2015 by the Bombay High Court while deciding the WP(C) 310/2014 titled **University of Pune, Ganeshkhind, Pune vs. State of Maharashtra**, that:

> *….The Courts should be extremely reluctant to substitute its opinions and views as to what is wise, prudent and proper in relation to academic matters in preference to those formulated by professional men possessing technical expertise and rich experience of actual day-to-day working*….

6. The NIC is the premier organization which has to be mandatorily consulted for dealing with any such data of national importance. Not only security of data but keeping citizen's private data secure is also important and an essential function of the NIC.

7. It is imperative to peruse the relevant provisions of the Right to Information Act, 2005, Information Technology Act, 2000 and Public Records Act to appreciate the exact nature and regime of the information under these Acts.

a) Right to Information Act***:*** According to Section 2(j) the right to information means the right to information accessible under this Act which is held by or under the control of any public authority..(iv) obtaining information in the form of diskettes…"

Section 2(f) information includes **emails**, contracts, etc.

Section 2(i) 'record' includes… (iv) any other material produced **by a computer** or any other device".

Section 3 Subject to the provisions of this Act, all citizens **shall have** the right to information.

Section 4 (1)(a) Every public authority shall (a) maintain all its records duly catalogued and indexed in a manner and the form which facilitates the right to information under this Act ….. (b)(ix) A DIRECTORY OF ITS OFFICERS AND EMPLOYEES… (xvii) update these publications every year..

Section 4(3) For the purpose of subsection (1) every information shall be disseminated widely and in such form and manner which is easily accessible to the public.

Section 4(4) All materials shall be disseminated taking into consideration the cost effectiveness, local language and the most effective method of communication in that local area and the information should be EASILY ACCESSIBLE, to the extent possible in ELECTRONIC FORMAT…

Explanation: For the purposes of subsections (3) and (4), 'disseminated' means making known or communicated the information to the public through notice boards, newspapers, public announcements, media broadcasts, the internet or any other means, including inspection of offices of any other public authority.

Section 8(1) Notwithstanding anything contained in this Act, there shall be no obligation to give any citizen:- (a) information, disclosure of which would prejudicially affect the sovereignty and integrity of India, the security, strategic, scientific or economic interests of the State, relation with foreign State or lead to incitement of an offence.

Section 8(2): Notwithstanding anything in the Official Secrets Act, 1923 nor any of the exemptions permissible in accordance with sub-section (1) a public authority may allow access to information, if public interest in disclosure outweighs the harm to the protected interest.

b) Information Technology Act, 2000: Failure to protect sensitive data attracts provisions of Section 43A of Information Technology Act 2000 as amended in 2008. Section 3 of Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 notified by Government of India on 11th April 2011 defines Sensitive

Personal Data SPD while Section 8 of these Rules defines Reasonable Security Practices and Procedures. Hence it is advisable that whenever any Department is collecting or keeping citizen data, Section 43A compliance Audit should be got done.

Section 43. Penalty and compensation for damage to computer, computer system, etc. If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network, or computer resource —

1. accesses or secures access to such computer, computer system or computer network;
2. downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
3. introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
4. damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;
5. disrupts or causes disruption of any computer, computer system or computer network;
6. denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means; (g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;
7. charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation to the person so affected.
8. destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;
9. steal, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;

Explanation.
For the purposes of this section:

1. "computer contaminant" means any set of computer instructions that are designed —
   - to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or
   - by any means to usurp the normal operation of the computer, computer system, or computer network;
2. "computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;
3. "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, daia or instruction is executed or some other event takes place in that computer resource;
4. "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.
5. "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

Section 43A*, Compensation for failure to protect Data:* Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.
Explanation: For the purposes of this section:

(i) 'body corporate' means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities.

(ii) 'reasonable security practices and procedures' means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures as may be

prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

(iii) 'sensitive personal data or information' means such personal information as may be prescribed by the central Government in consultation with such professional bodies or associations as it may deem fit.

Under this new law, *"sensitive personal data or information of a person"* means such personal information which consists of information relating to:

(i) password;

(ii) financial information such as Bank account or credit card or debit card or other payment instrument details;

(iii) physical, physiological and mental health condition;

(iv) sexual orientation;

(v) medical records and history;

(vi) Biometric information;

(vii) any detail relating to the above clauses as provided to body corporate for providing service; and

(viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise.

c) Duty to secure information for Security purposes: Negligence in implementing and maintaining reasonable security practices and procedures may make a person liable to pay damages. It is interesting to note that the Information Technology Act originally capped compensation claims at Rs 1 crore under section 43. This cap has now been removed. Compensation claims up to Rs 5 crore are now handled by Adjudicating Officers while claims above Rs 5 crore are handled by the relevant courts.

Section 72A provides imprisonment up to 3 years and fine up to Rs 5 lakh for disclosure of personal information in breach of a lawful contract.

Thus there is a duty to secure the information for security and privacy purposes. The Government of India has to make sure that the emails and websites of its ministries and departments do not get into the hands of other agencies within and beyond the country and for that it has to depend on the services of the expert national body like NIC.

d) Public Records Act, 1993: Section 4 says:

'*no person shall take or cause to be taken out of India any public records without the prior approval of the Central Government; provided hat no such prior approval*

shall be required if any public records are taken or sent out of India for any official purposes'.

8. Dealing with the main matter at hand, the most important point which emerges from the aforementioned discussion is that the information sought by the Appellant i.e. "…all email addresses details of Govt/Public authorities/ organizations maintained by NIC with up-to-date amendments therein" has been denied by the Respondent on the ground that the information is not in their custody, because the respective Ministries/departments which create the email addresses are the sole custodians and owners of the information. NIC has repeatedly stressed on the fact that they have no role to play in it since it is neither the owner nor the holder of the information. The Respondents state that they will have to procure all the information from the real owners of the information i.e. the various Govt departments and ministries spread all over the country. It is an admitted position in law that the obligation under the RTI Act is to make available or give access to existing information or information which is expected to be preserved or maintained. The information as sought by the Appellant in this case is not held in the same format by the concerned Respondent. Hence it would require collating the same and forming a compilation of a huge amount of information.

9. It is noted that the denial of information by the Respondent Public Authority coupled with their strong objection is based on their apprehension that dissemination of this form of information makes the cyber domain of the country at large vulnerable to any form of cyber attack. According to the Respondents' contentions there is high possibility of misuse of information in the form of release of all e-mail addresses of all the Public authorities in a consolidated CD form. The Respondents have repeatedly voiced their apprehension that such disclosure of information could make the Government internet network vulnerable to cyber attacks in the form of humungous amount of unwanted internet communications sent from fake IP address/es, choking the Government network and blocking access of the NIC servers. The repeated argument of the NIC for denial of information is based primarily on the apprehension of security threat to the systems set up nation-wide. The Respondent has even contended that even if it did possess the information requested by the Applicant, NIC would have to seek the views/suggestions of all the

third parties before parting with such information. The volume of the information is huge and Respondents have stated that they do not possess the resources to carry out the process as outlined under Section 11 of the RTI Act for seeking individual submission about disclosure of such quantum of information.

10. On a practical and possible logical front, the apprehension of the Respondent cannot be completely overlooked because availability and access to such wide array of information leaves scope for misuse and abuse of the same at the hands of any person. Apart from random mischief mongers or technical geeks or harmless but curious persons who may disrupt the entire cyber network by irresponsible handling of the information viz. the list of email id–s; the country actually runs a far greater risk of exposing itself to inimical, hostile nations, waiting to harm national security and interest by triggering a cyber attack or even worse, hacking into the systems and obtaining valuable confidential information of national importance. It is significant to note that Section 72A of the IT Act provides imprisonment up to 3 years and fine up to Rs 5 lakhs for disclosure of personal information in breach of a lawful contract. Thus there is a duty to secure the information for security and privacy purpose. The Government of India has to make sure that the emails and websites of its ministries and departments do not get into the hands of other agencies within and beyond the country and for that it has to depend on the services of the expert national body like NIC.

11. Moving ahead with the next limb of the matter, which emerged in the course of hearing held on 27/06/2014, it is noted that the Appellant has modified his request of seeking the information on a CD and agreed that mere uploading of the requisite information on the Respondent's website shall suffice his purpose.

12. In this context it is relevant to refer to the Email Policy of Government of India, released in October 2014 F. No. 2(22)/2013-EG-II, Ministry of Communication & Information Technology, Department of Electronics & Information Technology, version 1.0 which says:

The Government uses e-mail as a major mode of communication. Communications include Government of India (GoI) data that travel as part of mail transactions between users located both within the country and outside. (Para 1.1)

This policy of Government of India lays down the guidelines with respect to use of e-mail services. The Implementing Agency (IA) for the GoI e-mail service shall be National Informatics Centre (NIC), under the Department of Electronics and Information Technology (DeitY), Ministry of Communications and Information Technology. (Para 1.2)

Only the e-mail services provided by NIC, the Implementing Agency of the Government of India shall be used for official communications by all organizations except those exempted under clause no 14 of this policy. The e-mail services provided by other service providers shall not be used for any official communication. (Para 2.1)

13. The Official website of the Government and NIC provided following information under the heading GOV.IN Domain Registration**:**

(i) As per the new Internet Domain Name Policy released by the Department of Information Technology, NIC is the exclusive registrar for GOV.IN country level Domain Registration. GOV.IN has been reserved for registering domain names for all the Government Departments/ Institutions/ Organizations at various levels including Central Government, States & UTs, Districts, Blocks and Panchayats. To facilitate the GOV.IN Domain Registration, NIC has set up an exclusive website (http://registry.gov.in). The domain name registration policies, process and eligibility requirements have also been published on the site. The site also facilitates online registration of 'GOV.IN' Domain Names.

(ii) NIC has also been providing Domain Name Registration under NIC.IN as part of their Internet services since 1995 and has around 8000 domain names already registered. A majority of Government Ministries and Departments including State Governments and District Administrations have registered their domains under NIC.IN domain name. The Government sites which are hosted on Gov.IN Domain are being registered here. To facilitate the GOV.IN Domain Registration, NIC has set up an exclusive web site http://registry.nic.in

(iii) The official website of NIC also claimed that the NIC is extending comprehensive World Wide Web services (http://webservices.nic.in) to Central and State Governments,

Ministries & Departments in the areas of consultancy, web design and development, web hosting, value added web services for promotion of websites, enhancement of websites & training.

(iv) It is officially stated that the Government of India web directory is also being prepared by NIC. GOI Web Directory: - A one-point source to access all Indian Government Websites at all levels and from all sectors. "We welcome your participation in enhancing the Directory further and also invite your comments and suggestions for improvement." http://goidirectory.nic.in/index.php.

14. A detailed analysis of the various aspects of the case and the above discussion clearly indicates that the duty to secure the information is of utmost importance for security and privacy purposes. The Government of India has to make sure that the emails and websites of its ministries and departments do not become targets for anti-social elements within and beyond the country and for that it has to depend on the services of the expert national body like NIC, which is declared as the Implementing Agency (IA) as declared by policy document.

15. As per the avowed policy of the Government and duty of the NIC they have a self-declared obligation to facilitate the email services and prepare the email ids besides compiling the directories. It is the duty of the NIC to compile the directory of email ids, under the law and policy of Government of India. It is recommended under S.4 of Right to Information Act, 2005.

16. It is a matter of common knowledge that information as sought by the appellant is already available in the public domain at the click of button on separate websites of the respective Ministries and/or Departments. Citizens Charter/s already provided adequate information about the officials responsible for public dealing in various Government Departments/Ministries. Providing the list of all email ids in a CD format could pose a security threat as well as the risk of disruption of essential public services by making the information susceptible to misuse/abuse.

17. In these facts and circumstances, it is pertinent to note that the Central Government is currently working on a project to centralize all Government communications by creating a

communication hub on single platform. The Government of India Web Directory is a one-point source to access all Indian Government Websites at all levels and from all sectors. Suggestions have been solicited from the public for improvement of the same such that it serves the cause of the public better. Such a development, in larger public interest augurs well for the cause of transparency and also caters to the demand of the Appellant. Believing that directory is being developed under the vigilant and watchful Government set up, we require the aspects of national security and larger public interest and public reach shall be adequately addressed. The Commission also requires the directory meant for citizens at large must essentially be user friendly, and CPIOs/FAAs and officials posted in Grievance Redressal and Public Relations Offices etc. who deal with public at large, can also access the data easily. We require that as per appellant's request the NIC shall compile the GOI Web Directory at the earliest in larger public interest and all public authorities concerned shall expeditiously provide the necessary data to NIC to complete the task.

M. S. ACHARYULU
Information Commissioner

YASHOVARDHAN AZAD
Information Commissioner

BASANT SETH
Information Commissioner

Authenticated true copy:

(M.K.SHARMA)
Registrar

CC to
Mr. R K Jain

1512-B, Bhishm Pitamah Marg, Kotla Mubarakpur, New Delhi – 110003