From:
SarbaJit Roy
B-59, Defence Colony
New Delhi 110024
Tel : 2433-4262

To:
The Secretary,
Department of Information Technology,
Ministry of Communication & Information Technology
Electronic Sadan, 6 CGO Complex Lodhi Road
NEW DELHI 110003

BY HAND / EMAIL

DATE : 19-September-2005

Sir,

SUB: NOTICE OF MY OPPOSITION, AND SOME OBJECTIONS / SUGGESTIONS TO YOUR PROPOSALS DATED 29.AUGUST.2005 TO AMEND THE INFORMATION TECHNOLOGY ACT 2000.

Please take notice as under. In the event that you wish to deny / dispute the contents of this communication, you may do so in writing to me within 15 days from receipt, failing which I shall presume my contentions to be correct. I also inform you that I wish to be heard in person concerning these matters and also the enforcement of my Fundamental Rights affected in these matters and I hence seek an urgent appointment to be fully heard in person.

1) That on or about the 29.August.2005 you published on your website http://mit.gov.in a set of proposals purporting to be from an EXPERT COMMITTEE concerning amendments to the Information Technology Act 2000 ("the ACT"). You did also invite objections and suggestions to the same till 19.September.2005. That you did mischievously and in a discriminatory fashion publish these proposals only in your website in the form of a proprietary Microsoft 32-bit or higher document format which is unreadable on a vast number of computers such as mine. You made no efforts to publish a printed version of these proposals for distribution to affected persons, and neither did you publish the same in a portable document format which is easily readable across computer platforms, operating systems and font resources.

Consequently many persons such as me and others are forced to rely upon 3rd party sources concerning these proposals and are not able to reply as fully or effectively as we would wish to or at all.

2) That a perusal of the composition of this alleged Expert Committee reveals it to contain several lawyers, vested interests and person from lobby groups associated with computer industry in India, and does not sufficiently represent interests of persons principally affected by the ACT as mandated under section 88 of the ACT. In particular no provision has been made to seek inputs from victims of cyber crimes, or from the Police and other investigative agencies, or indeed from ordinary citizens who use the Internet ("netizens") or even from the Cyber Regulation Advisory Committee most of whose members were excluded from this so-called Experts Committee and which seems to have been bypassed. It is relevant that, as I am informed, NASSCOM or other members of this Expert Committee leaked the details of this dubious Expert Committee report to selected media such as the Times of India well before you published the said report on your website, Surely this constitutes an offence punishable under section 72 of the ACT when read with section 88(3) of the ACT and I trust that you will investigate and prosecute this aspect thoroughly.

3) That as you well know, the undersigned was the Complainant in Complaint No.1 of 2004 before the Adjudicating Officer under the ACT at Delhi who was appointed and notified by you. The said Complaint detailed information concerning commission of numerous cognisable offences of "hacking" punishable under section 66 of the ACT. As you well know a Government Department RBI was also Respondent in the said Complaint and liable for punishment under the section 66, and the said Department is member of the Cyber Regulation Advisory Committee constituted under section 88 of the ACT to advise upon the amendments to the ACT and other matters.

4) That to protect the offenders named in my Complaint, you did rapidly and mischievously with malafide intent, draw up a so-called "roadmap" a.k.a terms of reference for amending the ACT, which was widely circulated internally including to Secretaries of Information Technology Departments of the States who are *ex-officio* the Adjudicating Officers under the ACT. The said roadmap diluted and blunted the existing provisions of the ACT concerning the offences of Chapter XI of the ACT as well as the penalties under Chapter IX of the ACT. It is relevant that your handpicked Expert Committee now

mischievously and malafidely proposes to delete entirely the present section 66 concerning hacking with computers. That you are well aware that section 66 is the only effective deterrent section against cyber crimes in Indian Law and is a sufficiently strong protection to citizens of India, and it was based upon this section 66 alone that your Minister could assure Parliament that the ACT covered all types of cyber crime. That your proposals to modify the ACT and delete this section 66 etc. is dictated by the vested interests such as NASSCOM and their Foreign Members who have the free run of your offices – and which is most surprising considering the vital role your Department plays in protecting India's security.

5) That you have never bothered to ensure that the Central Government (which effectively means yourself – considering that yours is the nodal Department), in all these 5 years since the ACT has been in force, got prescribed the vast number of security procedures under section 16 of the ACT – thereby causing considerable harm and damage to me and numerous other persons. It is thereby foolish to expect that the Central Government (ie. yourself primarily) will notify or prescribe all the numerous other procedures and matters which the new proposals thrust everywhere upon this vague "Central Government" to do instead of your own Department which is clearly nodal in the matter and best suited to do so. Take note that if you persist with washing your hands of your mandatory duties, you have no business to change the law either.

6) That as you well know there was a rash of cyber crime in India about the time of my Complaint filed on 4.November.2004 and thereafter, some which I cite herein as:-

i) Arrest of CEO of Baazee.com Mr. Avneesh Bajaj,
ii) Hacking at Mphasis Pune
iii) Hacking in Karan Bahree incident,

And that the Central Government had been clearly informed well in time by my Complaint and also from other persons that hacking is rampant in India in the Banking and Financial sectors of India, carried out by organised gangs and cartels of persons with Foreign links and connections. Yet you and your appointed Officers made no absolutely effort to investigate such informations, causing our proud nation to be internationally disgraced in the Karan Bahree Hacking incident in June 2005 despite having had over 7 months to track down these cyber

criminals openly operating under your nose. That you further encourage and permit these offences to be secretly compounded by your bureaucrat officers in a discretionary fashion, instead of getting them prosecuted as criminal offences with exemplary punishments, so as to sweep India's endemic cyber crime problems under the carpet – and in fact the ACT drafted by you avoids all mention of the controversial words "cyber crime".

7) That you were afraid of the international media publicity attendant if the thousands of international victims of cyber crimes being committed in India were to seek large damages and penalties in India, and hence you privately instructed the Officers under you such as Adjudicating Officers, and Controller to dismiss all reports / complaints concerning these crimes from the victims / persons affected by these crimes as permitted in the ACT, and to only entertain Complaints / Reports from the Owners of computers who were unlikely to complain. In this connection your Officer - the Deputy Controller of Certifying Authorities one Dr.K.K.Bajaj (who under section 28 of the ACT is the prime investigator of such matters) gave a mischievous interview on NDTV denying that he would entertain such complaints or would investigate the same, and that Police should be contacted instead. I am informed that Dr.Bajaj, who by all accounts is an exceedingly efficient and qualified officer, has resigned from your Department / Government services due to personal reasons.

8) That you mischievously and willfully refrained from constituting the Cyber Regulation Appellate Tribunals mandated under section 48 of the ACT. That in fact your Minister had assured Parliament as far back as 2002 that the said tribunals would be set up when need arose, however, you took no steps to set up the same forthwith upon my Complaint being filed. As a consequence my said Complaint of Hacking (which is the first and only such Criminal Complaint under section 46 of the ACT) could not be transferred to the Magistrate to prosecute the offenders (including Government Officials on your Committees) who have committed / abetted the cyber crimes of "Hacking", and in fact allowed some of them were allowed to flee the country due to your appointed Officer's suspicious lethargy to investigate my Complaint. Also, I have no provision to appeal the Order in my case, since the mischievous remedies suggested by you, under section 62 of the ACT or Article 227 of the Constitution, are inapplicable and would not be maintainable.

9) That to further cover up your failure to set up the Cyber Regulations Appellate Tribunals, you secretly instructed the Adjudicating Officer, appointed by you, hearing my Complaint to dismiss my Complaint without reference to the merits of my case and to adjudicate my Complaint on the basis of the proposed amendments to the ACT vide the aforesaid “roadmap” and not on the basis of the law in force at the time. Hence, the entire proceedings in my Complaint carried out by your appointed Adjudicating Officer was a farce and violated principles of natural justice at every step. It is relevant that the ACT has been mischievously drafted by you to deny natural justice during adjudicating proceedings.

10) That I have no faith in your Department with reason, and am aggrieved with the malafide and mischievous proposed amendments to the ACT as made out by your alleged Expert Committee. In connection with these proposals I say broadly:-

i) The said proposals seriously weaken and dilute the strong provisions of the existing ACT, being overtly partial to the business interests and lobbies who exercise considerable influence over your Department,

ii) The proposals make a mockery of the United Nations model law of 1997 which was the basis for the ACT.

iii) There is excessive delegation of powers proposed now to unspecified departments of Central Government, excessive reliance upon industry self regulating bodies (which is but a thinly disguised permission for lobby groups and bagmen to freely roam the halls of your Department), and an overall abrogation of responsibility concerning your Department and the exercise of powers conferred by the ACT.

iv) There are too many knee-jerk or fire fighting exercises being attempted to be carried out in response to individual incidents by these proposals. Such kind of Band-Aid quick-fixes serve no purpose since, as you well know, the problem is not with the existing provisions of the ACT but rather with the incompetence or inexperience or corruption of the persons enforcing the ACT.

v) No attempts have been made to tackle common cyber problems faced by netizens such as spamming, spyware,

adware, P2P, email frauds such as phishing, dns cache poisoning, cyber stalking, defamation and extortion, bandwidth hijacking, false databases, database mining, tracking cookies, on-line privacy, data protection issues etc. These are most serious deficiency and you are obviously incompetent to draft any meaningful legislation on the same, whereas India has no shortage of capable persons who are drafting these matters for Foreign multi-lateral operations. By way of example I advise you to study fine works on these matters by a Mr.Suresh Ramasubramanian from Chennai for the Secretary-General of the OECD and others such as UNDP, the links for which are :-

http://www.oecd.org/dataoecd/5/47/34935342.pdf

http://igov.apdip.net/ORDIG_releases_paper/

and which I am not reproducing here in interests of brevity, but may rely upon these documents subsequently.

11) That I am listing out below some of my objections and suggestions to the proposals, with a faint hope that good sense will prevail upon you and your Department. I specifically inform you here that as a citizen of India, I am entitled to the protection of strong laws and the expectation of International agreements, treaties and covenants to beneficial protection of these laws as Fundamental Rights / Directive Principles, and I shall fully protect and get enforced any violation / abridgement of these my Constitutionally conferred Rights.

12) That I object to the changes of section 1(4). I say that all exclusions must be specified within the ACT itself as hitherto.

13) That I say the definition of "**appropriate Government**" at 2(e) is imprecise concerning the State Governments and requires tightening

14) That I say the definition of "**asymmetric crypto System**" at 2(f) is limited only to digital signatures, whereas it can be expanded to some other authentication methods also.

15) That I say in the definition of '**computer**" at 2(i) the words "connected or related to" may be altered to "concerned with or related to". Also the word "storage," may be amended to "storage, memory, power supply, protection, communication,"

16) That I say the proposed definition of '**computer network**" at 2(j) to also include computer systems is illogical and may lead to farcical situation of 2 dumb terminals if interconnected being considered as computer network. That I further say that clause 2(j)(i) is imprecise and limiting and would be better written as "the use of any means allowing data interchange".

17) That I say the proposed definition of '**Cyber Cafe**" at 2(nn) is too wide and vague. In fact there is no need to define Cyber Cafes at all, as I say that such classification for the purpose of exempting Cyber Cafes from penalty and prosecution under the ACT is discriminatory, arbitrary and illegal. If at all such classification is required it would be better written as "a semi-public premises where access to the Internet is provided against payment or consideration"

18) That in 2(o), it would better read as "…which is being prepared or has been prepared…".

19) In 2(t), please specify "as the Central Government shall prescribe"

20) I object to "message" being included explicitly as information at 2(v). It is better if instead "electronic record" is substituted for "message'. Furthermore since 'message" has nowhere been defined, addition of 'message" here will create confusion with the "message' presently contained within definition of "intermediary". Also the various definitions of terms such as of "information" in the ACT must be better harmonized with the similar definitions / usages in the Right to Information Act of 2005 – which you seem to have overlooked.

21) The definition of "intermediary" at 2(w) is too vague and would be better written as "means any authorised service provider (qv. note to section 6) who under lawful agreement or contract receives, stores or transmits electronic record(s) without modification on behalf of another person, but does not include an originator". Other Service Providers should be excluded from definition of intermediary. I caution you that this definition is directly concerned with the unique facts and circumstances of my Complaint which are very well known to you, and that you are tampering the law here to protect persons close to you.

22) I forcefully object to the definition of "subscriber" at 2(zg). There are numerous places in the ACT and the proposals where the term

"subscriber" is used (say concerning intermediaries) which have nothing to do with digital or electronic signatures and are obviously referring to "subcribers" of telecom, internet, broadband services etc. as say defined in the TRAI ACT etc. This definition must be substantially rewritten and amended suitably.

23) I object to the definition of "verify" at 2(zh). Presumably this concerns "authentication". Also it must be appropriately specified that in event any electronic record is not affixed with electronic signature, this in no way implies that said record is false or affects its legality or admissibility OR denies its verification by other means. An example of this being telegrams.

24) That in section 6 concerning filing of records and applications with Governments and agencies, the proposals may need to be harmonised with Acts such as Right to Information Act 2005 wherein another class of "Competent Authorities" such as President of India, Chief Justice of Supreme Court, Speakers of Houses of Parliaments etc are also covered who can frame their own forms and procedures. Also "delivery of service" must be distinguished from "service of process". Since Right to Information Act 2005 comes into effective force from October 2005, it may be ensured that the said RTI ACT is not delayed because of these mischievous amendments you are now belatedly proposing.

25) I forcefully object to the proposed section 10 concerning "Formation and Validity of Contracts". Firstly, the ACT ought only to be an enabling provision for other laws such as the Contracts Act or suchlike as suggested by the preamble to the ACT concerning E-commerce. Secondly, your handpicked Experts Committee is not competent to delve into these areas, which should have been done by the Cyber Advisory Committee which seems to have been bypassed. Thirdly, the proposals concerning these Electronic Contracts are unilaterally fascist, unconstitutional, discriminatory and violate all principles of well settled contract law, and have been included solely to benefit vested corporate interests like NASSCOM. If at all such inequituous legislation is required it should be written as follows:-

"a) In the context of contract formation, <u>if previously mutually</u> agreed by the parties, an offer <u>or</u> the acceptance of an offer may be expressed by means of an electronic record <u>authenticated by the digital signatures of all parties or of the concerned party</u>.

b) Where electronic records are used in the formation or registration of a contract, such contract shall not be denied validity or enforceability on the sole ground that electronic records were used for the purpose."

26) I strongly object to inclusion of the word "prescribed" in section 14 concerning security procedure for electronic records. For 5 years now your Department and/or the Central Government have sat upon your collective backsides and not prescribed any substantial security procedures for commercial transactions in areas such as Banking, Finance, E-commerce etc. Furthermore the entire "Convergence Bill" has been consigned to the cold-storage. By adopting a myopic and Departmentally convenient stand you are denying numerous citizens of India the protection of India's strong laws. I caution you that this mischievous inclusion of "prescribed" is directly concerned with the unique facts and circumstances of my Complaint which are very well known to you, and that you are tampering the law to protect persons close to you thereby violating my Fundamental Rights.

27) That I object to wording of section 15 proposed. It should read as "… by the parties concerned or where there is no such agreement prescribed by the Central Government, …"

28) That I forcefully object to the new section 16 being proposed. There is absolutely nothing wrong with the old section. I strongly object to the mandatory inclusion of any allegedly self regulating industry bodies. This entire new clause 16(2) has been thrust by NASSCOM to legitimise NASSCOM's industry wide blacklists of employees and other cartel-ian measures which NASSCOM is proposing whilst portraying themselves to be the self regulating body for computer and IT industry. I caution you that this mischievous deletion and tampering of section 16 is directly concerned with the unique facts and circumstances of my Complaint which are very well known to you, and that you are tampering the law here to protect persons close to you thereby violating my Fundamental Rights. I warn you that by attempting to dilute the mandatory nature of this section from "shall" to "may" you are exposing the real agenda of your handpicked Expert Committee controlled by NASSCOM and their chosen lawyers– which is to deny Indian citizens their Fundamental Rights to the equal protection of India's Laws.

29) I strongly object to any dilution of the Controller's investigative powers under section 28 by the additional phrase "under this Chapter". When under section 29 the Controller can still access computers and data concerning contravention of any provisions of the ACT, why is he now being limited to only this Chapter under section 28. If not the Controller, then who is empowered to investigate contraventions of the entire ACT now that role of Police has also been neutered by later proposals? Surely you are not seriously proposing that mere *ex-officio* Adjudicating Officers should investigate everything in addition to their other duties they are over-burdened with? Are there any replacements proposed to the Controller - who have such equally sweeping and over-riding extraordinary powers of investigation as under the present section 28? I caution you that this mischievous proposed modification to section 28 is directly concerned with the unique facts and circumstances of my Complaint which are very well known to you, and that I was constrained to file my Complaint with the Adjudicating Officer at Delhi solely because your Dy. Controller (Security) Dr.K.K.Bajaj refused to investigate my information under section 28 and referred me instead for Adjudicating Proceedings when he knew full when that the Cyber Regulations Appellate Tribunal was non-existent and my Complaint could thereby not be transferred to the Magistrate.

30) I strongly object and take exception to the amendments proposed for section 43. You are well aware that this section is directly concerned with my Complaint and that your mischievous proposals are with a view to frustrate my Complaint in particular and to dilute the ACT in general. In connection with the amendments of this section I say:-

i) I object to substitution of "computer resource" everywhere in place of "computer, computer system or computer network". This amendment is designed to benefit software companies and vendors like NASSCOM's membership who are primarily Foreigners. This will lead to all sorts of confusion and litigation concerning ownership of embedded software and licenced software within devices and IPR and copyright issues. I may point out that in 1999 computer software was specifically included from coverage under this section, what has changed now, is it the fact that these Expert Committee proposals have been drafted by NASSCOM (an association and lobby group for software vendors) and their lawyers and merely rubber

stamped by you, or are there extraneous considerations involved?

ii) What is meant in 43(1)(d) by computer data base residing within such computer resource, isn't computer database already included within computer resource?

iii) Please clarify what the role of this section is when damage to computer etc. takes place when there is a conflict between the "owner" of computer and "person-in-charge" of computer and one causes damage to the other. As an example, A hires a computer webserver system from B (the owner) – there is some dispute between them and A refuses to pay the installments due, whereupon B (the owner) without following due process activates a secret logic bomb that deletes critical files of A (person in charge) and also of numerous other persons storing files on the said webserver. Who has the locus to file complaint for compensation? I again caution you that these mischievous proposed modifications to section 43 are directly concerned with the similar unique facts and circumstances of my Complaint which are very well known to you, and that you have only proposed these so that every Indian victim and also numerous Foreign victims of Cyber Crimes has no recourse in law (in view of section 61 of the ACT) to damages and compensation, and are instead forced to compound and settle these offences by your appointed bureaucrat officers in a corrupt fashion.

iv) What is intended by your vaguely defined terms like "reasonable security practices and procedures" in 43(2). Who in the Central Government is going to prescribe such procedures and in what time frame, and what if there are no such security practices or procedures laid down? Why is it only limited to bodies corporate, why have societies, trust and NGOs etc. been left out? Why is this clause limited to persons owning or operating computer resources and not also applicable to persons transmitting, storing or receiving electronic records in any form or also to those who outsource such data. Who is going to investigate these matters and find the parties to be negligent? Surely the burden of proof cannot be placed on victims of these cyber crimes. Why are these matters also not being simultaneously treated as criminal offences under the

ACT? Why are damages not awardable upon persons who willfully disseminate personal data from computer resources they own or operate such as organised rings of computer hackers or illegal credit information bureaus? Will such damages be in addition to those payable for similar contraventions under say the Credit Information Companies Regulation Act 2005, and will this not lead to confusion and multiple litigation? Why are you repeatedly involving self-regulatory bodies of the industry. What is the situation where there are several different self-regulatory industry bodies with different sets of practices and procedures? For example for the Internet, would the self-regulatory industry body be some Association of ISPs or would it be TRAI or the DoT or TDSAT or the W3 consortium or ICANN or some association of Hackers? Please isolate yourself and your Department from industry associations and lobbyists like NASSCOMs and their ilk. It is an open secret in cyber law circles that your Department does not have the technical staff or capability to draft any meaningful legislation on cyber regulation matters and which is why you had delegated this process of revamping the ACT to NASSCOM and their lawyers, who have thoroughly abused your hospitality in this sordid affair of ACT revision. I also object to the weak and meaningless definition of "sensitive personal data or information" especially since all such information has to be first prescribed by Rules under the ACT by the Central Government – which given your track record in the past 5 years is highly unlikely – and again you have dragged in these so-called self-regulatory industry bodies like NASSCOM who are nothing but lobbyists and carpetbaggers for software industry. This entire exercise concerning redrafting of section 43 is a case of deception and misrepresention – wherein you portray that the laws are strong – but you thereafter dilute and render impotent these clauses in the definitions and Rules.

31) Insofar as section 46 is concerned, I say:-

(i) Please clarify if Adjudicating Officers's role is limited only to under this Chapter plus section 72 (as suggested by footnote), OR is it now extended to the entire ACT. Please also fully clarify if the Adjudicating Officers role is limited to cases of payments of penalty or compensation or does it also extend to

cases requiring punishment under the present Rules. You are well aware of the significance of these aspects with respect to my Complaint and also your mischievous roadmap - which is now exposed in the impugned proposed phrase "which renders him liable to pay penalty or compensation," and to which phrase's inclusion I take strong exception.

(ii) That proceedings before the Adjudicating Officer should also be governed by principles of natural justice, and that lawyers or legal practicioners should be excluded from these proceedings.

(iii) If role of Adjudicating Officer is now to cover the entire ACT, then there should be independent full time such Officers and not ex-officio bureaucrats who cannot devote time. In my own Complaint as you well know, all parties apparently appeared, no adjournments were asked for by anyone, all pleadings and rejoinders were filed promptly, and yet it took your Officer 7 months just for admission of the matter - whereas the ACT specifies that entire matter must be disposed of in 6 months. And this too before an Adjudicating Officer with only 2 pending Complaints.

32) That section 57(3) should be amended to read as:-

"Every appeal under sub-section (1) shall be filed within a period of forty-five days from the date on which a copy of the order made by the Controller or the adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed not exceeding double the fees deposited in the lower forum. Provided that the Tribunal may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days. Where the Tribunals were not constituted the time for filing appeals shall be counted from such date as the Tribunal determines, or the prospective appellants may avail their remedy under section 62 or under Article 227 of the Constitution."

33) That I applaud the decision to delete / move section 63 concerning compounding of offences. I am also unable to find this section 44A to which these matters have been shifted. Are you referring to section 80A perhaps? If so, I shall voice my comments on this there.

34) That insofar as section 65 is concerned I say:-

i) does the term “conceal” include encryption? Does the term “conceal” include obfuscation of code also? Please fully define “conceal” for the purposes of this section, you have already done so for IPC purposes.

ii) Please delete the phrase “when the computer source code is required to be kept or maintained by law for the time being in force”, since this will truly give Indian software developers an effective protection. Furthermore restricting the protection of this strong clause only to Government software code is discriminatory, arbitrary, high-handed and unconstitutional.

iii) Does this clause sufficiently protect the “look and feel” of software also, concerning “design and layout” etc.?

iv) Please increase the imprisonment to 7 years and the fine upto one crore rupees.

v) Please specify that this offence is cognisable notwithstanding anything in the CrPC.

35) That concerning section 66 on "Hacking with Computers" I say:-

i) That you have wrongly, and with malafide intent proposed to delete the existing section 66 entirely. That you have done this so as to frustrate my ongoing Complaint concerning this section.

ii) I caution you that if you persist with your foolish proposal to delete or dilute the existing present section 66 I shall view this as an abridgement / unreasonable restriction of my Fundamental Rights and act accordingly to get these Rights enforced.

iii) I call upon you to retain the existing section 66 in toto, and I further call upon you to strengthen this present clause by suitable amendments as follows:-

“66. Hacking with Computer System

(1) Whoever, with intent to cause or knowledge that he is likely to cause damage or wrongful loss to any person or the public, destroys or deletes or alters or conceals or transmits or publishes any information residing in a computer resource, or diminishes its value or utility, or affects it injuriously by any means, commits hacking.

(2) Whoever commits hacking shall be punished with imprisonment up to 7 years, or with fine which may extend to twenty five lakh rupees, or with both.

(3) Notwithstanding anything contained in the CrPC or any other law, the offence punishable under this section shall be deemed to be cognisable."

The new Computer related offences proposed instead at section 66, may be incorporated as a new section 66A, since these concern damages to computer systems and networks wherein harm and damage is cause to computers and hence require lesser sentence of two years, as against the present section 66 concerning damages and harm caused to persons with computers (hacking) and which deserve higher punishments.

36) That concerning section 67, I say:-

i) This entire section as proposed deserves to be scrapped and all these matters may be better incorporated into the Indian Penal Code at the appropriate section 292 etc. as minor enabling clauses under the ACT. The nature of the tool used to commit the crime should have no bearing upon the crime itself or the punishment thereof. Hence I say obscenity, pornography etc. are already well covered under the existing IPC which is a time tested body of law, and these kinds of publicity oriented knee-jerk tinkering with the laws of India as your alleged Expert Committee is proposing well exceed the mandate and competence of your Department. I also bring to your notice that such differentiation concerning obscenity in the electronic form is discriminatory and arbitrary – why now two years and not five or why now 3 years and not for life etc.

ii) That in place of section 67, you may devote your attention to specific and sophisticated cyber crimes such as spamming, spyware, adware, P2P issues, email frauds such as phishing, dns cache poisoning, cyber stalking, cyber defamation and extortion, bandwidth hijacking, false databases, database mining, tracking cookies, on-line privacy, data protection issues etc in its place.

37) That insofar as section 68(A) is concerned, I say that there is no need for this section at all, which seems to have been hastily tacked on to assuage constant criticism of your Department concerning permissibility of encryption, 128 bit, 40 bit etc which is under the DoT. This clause as it stands is meaningless and hollow, and would be better incorporated under section 16. Also why is encryption only being considered for e-governance and e-commerce, and not for areas like Banking and Finance. My Complaint had well gone into this aspect and thoroughly exposed your failure to notify the necessary security procedures under section 16.

38) Insofar as section 69 is concerned, I say:-

i) Till such time as Central Government (surely you do not mean the President of India personally !) is satisfied to do all the things required under this section, the Controller may be allowed to carry on as at present. You are making a big mistake by excluding commission of cognisable crimes from this facility. If someone is going to be murdered by conspiracy via steganography, or hijackers are planning their conspiracy over e-mails surely someone must be designated to get decrypted the information and not some vague Central Government – alternatively list out all the agencies which can do so in a schedule to this ACT. Why are you repeatedly denying Indian Citizens the protection of strong laws – which even countries like USA are scrambling to catch up with ours – is it because of extraneous considerations from lobbyists and unfriendly nations opposed to India's security? Why are you passing these strong laws so belatedly – is it because your Ghitorni faciities are not yet fully ready? I OPPOSE ANY PROVISION OF LAW THAT ALLOWS / PERMITS INTERCEPTION OR MONITORING OF ON-LINE ACTIVITIES OF INDIAN CITIZENS WITHOUT THEIR KNOWLEDGE, OR RESTRICTS/DENIES THEIR RIGHT TO PRIVACY IN THEIR HOME OR PERSONAL AFFAIRS.

39) Insofar as section 72(2) is concerned, I fully support this clause and suggest it can be made stronger by deletion of the phrase “Save as otherwise provided under this ACT”. Furthermore, the term “subscriber” as used here has nothing to do with signature certificates – or does it? The clause would better written as:-

“If any intermediary or service provider has gained access to any electronic record or other information, and thereafter with intent to cause injury discloses or permits to be disclosed without necessary consents such information or record, either partially or fully, to any other person, such intermediary or service provider shall be liable to pay damages by way of compensation not exceeding Rs. 25 lakhs to every person so affected.”

40) That insofar as proposed section 72(3) is concerned, this should be deleted in toto, since it is an exceedingly badly drafted piece of legislation and will also make India the laughing stock abroad. Such kind of pathetic legislation is not even found in Islamic countries and harks back to era of sanitary inspectors. I reiterate that these matters are best left to the Indian Penal Code and CrPC, and your suspicious tinkering with these laws via the ACT deserves to be investigated appropriately. Who is going to measure the female breast from the top of the areola, you?

41) That insofar as section 78 is concerned, this would be a good place to specify that all offences under Chapter XI are cognisable and non-bailable and may be reported / investigated under the CrPC. Furthermore that considering the explosion and escalation of cyber crime especially after the enforcement of the ACT since 2000, that the requirement of investigation by DSPs and above may be deleted.

42) That considering section 79 I say:-

i) The entire clause 79(2) is vague and redundant, and may be deleted. Incidentally this clause may cause more problems than it will solve.

ii) Concerning 79(3) please specify “expeditiously”, do you mean “forthwith” or “immediately” ? You cannot have such vague drafting concerning criminal matters.

iii) Concerning explanatory definition of "intermediary" in this section, you may please delete the clause explaining the various type of intermediaries, since this serves no purpose and will cause further confusion. In any case, what is so special about on-line auction sites, market places and cyber cafes etc. that they deserve to be exempted. Do you have any evidence or basis to say that such on-line markets etc. are honest and above board? Please distinguish the procedurally incorrect arrest of Mr. Avneesh Bajaj from the activities of his company. Surely it will create administrative problems if every time the Central Government or its agencies have to intervene to get items deleted from these websites, the President of India has no time for all this and there will be great delay causing aggrieved persons like me to repeatedly approach the courts and clog up the judicial system due to your vested drafting.

43) That insofar as section 80 is concerned, I am Appalled that you propose to delete the present section concerning search and seizure powers of Police Officers. This ineptitude on your part will not go unchallenged. What are you trying to portray – that India is a great place for all sorts of cyber criminals and that Foreigners should transact their dirty IT businesses here which they cant do in their own countries – without any fear of investigation or prosecution. Why has Mr.Karan Bahree not yet been apprehended? If the Police will not apprehend him and his gang of hacker associates then who will? What influence has NASSOM brought to bear upon your Department that you will not track down and prosecute such persons despite my specific Complaint to your appointed Officers to do so? And in any case why have you permitted NASSCOM to train Police Officers in cyber crime investigation, don't you have any competent persons under you to do so? Why are other Industry Associations like FICCI, CII, ASSOCHAM, MAIT, CETMA etc. not being similarly associated in these cyber crime matters (say by being involved in redrafting the ACT) and why is NASSCOM alone being favoured by you? It is a sad day Sir when the regulatory departments of government systematically encourage the fraternisation of organised offenders with the investigative and enforcement agencies. I call upon you Sir, not to delete or dilute any of the provisions of the existing section 80.

44) That insofar as the proposed section 80A concerning compounding of offences is concerned, I call for the deletion / substantial modification of this entire section, and I say as follows:-

i) I am greatly disturbed to be informed from cyber-law circles that all sorts of discretionary compounding (involving corrupt practices) of cyber crime offences is being carried out under the ACT. Ordinarily I would have paid no credence to such talk, but the suspicious lethargy of your Department and your appointed Officers to apprehend persons such as the numerous suspects in my Complaint, Karan Bahree and his associates leads me to suspect there may be some truth in these whispers. Hence I am absolutely opposed to compounding of criminal offences in the present manner. Please pay heed to the victims of these cyber crimes, I am appalled that there is no safeguard provision to take the consent of the victims of cyber offences before compounding and in fact the victims of these crimes are not even informed that the matters have been compounded and will discover this like me only at the last moment when the Adjudicating Officers / Controller will dismiss their Complaints on false grounds after indulging in these corrupt practices.

ii) Furthermore the Adjudicating Officers / Controller are looking into Contraventions generally and not the Offences. So where does the question of compounding of Offences by these Officers arise? Why are the Magistrates not involved in this process? These are not some minor traffic offences to be compounded for Rs.100, but these involve crores of rupees, and there must hence be adequate safeguards against misuse of this compounding facility by possibly corrupt bureaucrats.

iii) I have no objection to plea bargaining to save time, wherein the Respondents to a Complaint may make a settlement offer to the affected persons by some sort of formal provisions of law in the ACT. In fact I suggest such procedures may be considered.

iv) Also, I am concerned sufficiently to inform you that a buzz in certain circles is that the PMO and your Minister being concerned with India's international image had resulted in the tracking down of the hackers / intermediaries in the Karan Bahree affair but these offences were compounded instead (in corrupt fashion) and the cyber criminals walk about freely to

stalk new victims such as the Australian Broadcasting Corporation. As you are well aware I was the victim of hacking of banking data of both British and Australian Banks, and hence if these allegations of compounding are true I would be most aggrieved.

45) That insofar as section 81 is concerned, I am opposed to the inclusion of section 81(2), since you are unnecessarily complicating the ACT which hitherto has been a simple and linear ACT being based essentially upon the UN model law and the Singapore Law. Please entirely delete the proposed clause 81(2) as there is no requirement for this clause.

46) That insofar as section 85 concerning offences by Companies is concerned, I am appalled by your proposed changes. Surely now that a Constitution Bench of the Supreme Court, in a matter (CA 1748/1999) involving the same Respondents of my Complaint, has recently found that there is no bar to prosecution of companies for imprisonment, one would have expected this section 85 to be further strengthened. Instead you have turned the concept of Corporate liability upon its head and do not seem to have appreciated the inherent difference between a "natural person" and an "artificial person". How can the victims of cyber crime determine which particular person(s) in the company was the actual offender? Why are concepts like “unless it is proved”, “connivance”, “failed to prevent such contravention” being dragged in belatedly to cloud the issue and dilute the bite of this section? Why is there again confusion in your mind and the drafting between “contravention” and “offences”, surely these terms are not interchangeable? The existing provision is analogous to numerous other sections of corporate law where the company or some designated person takes the blame / suffers the consequences of corporate crime. It is clear as daylight that NASSCOM and the other lobbyists who walk your corridors have again unduly influenced someone in your Department to turn the law on its head, and that no heed has been paid to average netizens and the victims of cyber crime. I caution you that these proposed modifications to section 85 are directly concerned with the unique facts of my Complaint and that you are tinkering with this law to shield persons known to you. I may also inform you Sir, that the persons who were upset with Mr.Avnish Bajaj’s arrest did not hold the ACT responsible but rather the incompetent and inept investigative and

enforcement machinery. Hence if the law is changed in the illegal manner you propose, it shall not go unchallenged.

47) That insofar as section 87 is concerned, I reserve the right to separately and later comment / object to this section since it concerns virtually every matter I have already covered.

48) That insofar as section 90 is concerned, I object to the phrase "Subject to any rules made by the Central Government," and call for its deletion.

49) I fully support the new proposed amendments to the Indian Penal Code. In particular I applaud section 118, 119, 120, 417A, 419A proposals. However:-

i) There should be no scope for confusion anywhere concerning "design" under the IPC and "design" as applicable to say product design.

50) That insofar as proposals for Indian Evidence Act amendments are concerned:-

i) Please clarify for 45A if it is Examiner of Digital Evidence or Electronic Evidence.

I hope Sir that you will carefully note the contents of this communication, and ensure the protection and enforcement of my various Fundamental Rights as a citizen of India. I again remind you that should you wish to dispute or clarify any matters of fact or opinion or law conveyed herein I call upon you to communicate the same in writing to me within 15 days of today. Alternatively I am always available to clarify matters in person, and you may give me an appointment with at least 72 hours prior notice. I also wish to appear in person before the Cyber Regulation Advisory Committee or any other relevant Committee or Group to further explain my views on these matters, and you may instruct accordingly.

Yours faithfully,

(SarbaJit Roy)