S E C T I O N … … … …

IN THE SUPREME COURT OF INDIA

(ORIGINAL /CRIMINAL /CIVIL/APPELLATE JURISDICTION)

WRIT PETITION (CIVIL) NO……..2013

(Under Art. 32 of the Constitution)

IN THE MATTER OF:-

PROF. S.N. SINGH …PETITIONER
PATRON, BANAANAA.COM

VERSUS

UNION OF INDIA …RESPONDENT

INDEX

SR. NO.	PARTICULARS	COPIES	PAGE NO.	COURT FEE
1.	W.P. with Affidavit	1 + 3	1-25	
2.	Annexures P-1 to P- 8	1 + 3	26-49	
3.	Application for ad-interim directions	1 + 3	50-52	
4.	Urgency Affidavit	1 + 3	53-55	
5.				
6.				
7.				
8.				
9.				
10.				
			TOTAL	

Certified that the copies are correct

Filed on: 18.06.2013 **Filed by**

Drawn by- **Virag Gupta, Advocate**
Managing Partner, RTI Legal, New Delhi

(Rajeev Kumar Singh)
Counsel for the Petitioner
Code No. …..
17, Central Lane,
Bengali Market, New Delhi-110001

V A K A L A T N A M A

I N T H E S U P R E M E C O U R T O F I N D I A

(ORIGINAL /CRIMINAL /CIVIL/APPELLATE JURISDICTION)

WRIT PETITION (CIVIL) NO…….2013

IN THE MATTER OF:-

PROF. S.N. SINGH …PETITIONER
PATRON, BANAANAA.COM

VERSUS

UNION OF INDIA …RESPONDENT

I PROF. S. N. SINGH**, PETITIONER** in the above Petition do hereby appoint and retain Rajeev Kumar Singh, Advocate of the Supreme court of India, to act and appear for me in the above Petition and on my/our behalf of conduct and prosecute (or defend) or withdraw the same and all proceedings that may be taken in respect of any application connected with the same or and decree or order passed therein, including proceedings in taxation and application for review, to file and obtain, return of documents and to deposit and receive money on my behalf in the said Petition and in the above matter. I/We agree to ratify all acts done by the aforesaid Advocate, in pursuance of this authority.

Dated this the 18 day of June 2013

Accepted and Identified

.....
Petitioner

MEMO OF APPEARANCE

To,
The Registrar,
Supreme Court of India,
New Delhi

Sir,

Please enter my appearance on behalf of the Petitioner in the mentioned above.

Dated this the..... …….day of ……..…….2013

Your Faithfully

(Rajeev Kumar Singh)
Counsel for the Petitioner
Code No. …..
17, Central Lane,
Bengali Market, New Delhi-110001

Dated:..06.2013

New Delhi

IN THE SUPREME COURT OF INDIA

[CIVIL ORIGINAL JURISDICTION]

WRIT PETITION (C) NO. /2013

IN THE MATTER OF:-

PROF. S.N. SINGH ...PETITIONER
PATRON, BANAANAA.COM

VERSUS

UNION OF INDIA ...RESPONDENT

WITH

I.A.No. of 2013

APPLICATION FOR AD-INTERIM DIRECTIONS

PAPER BOOK

(For index kindly see inside)

COUNSEL FOR PETITIONER: RAJEEV KR. SINGH

INDEX

A

LISTING PROFORMA

IN THE SUPREME COURT OF INDIA

1	Nature of the matter		Writ Petition(Civil)
2	i. Name(s) of Petitioner(s)		Prof. S.N. Singh
	ii. e-mail ID		s_nsingh@hotmail.com
3	i. Name(s) of Respondent(s)		UOI
	ii. e-mail ID		N.A.
4	Number of case		Writ Petition [c] No._____/2013
5	i Advocate for Petitioner		Rajeev Kumar Singh
R.	ii. e-mail ID		adv_rajeevs123@yahoo.co.in
6	i. Advocate(s) for Respondent(s)		N.A.
	ii. e-mail ID		N.A.
7	Section dealing with the matter		PIL
8	Date of the impugned Order/Judgment		N.A
8A	Name of Hon'ble Judges		N.A.
8B	In Land Acquisition Matters		N.A.
i)	Notification/Govt. Order No.(U/s 4.6) Date Issued by Centre State of		N.A.
ii)	Exact purpose of acquisition & village involved		N.A.
8C	In Civil Matters		
i)	Suit No., Name of Lower Court		N.A.
ii)	Date of Judgment		N.A.
8D	In Writ Petitions:		
	"Catchword" of other similar matter		N.A.
8E	In case of Motor Vehicle Accident Matters		
	Vehicle No		N.A.
8F	In Service Matters		N.A.
i)	Relevant service rule, if any		
ii)	G.O./Circular/Notification, if applicable or in question		
8G	In Labour Industrial Disputes Matters		N.A.
	I.D. Reference/Award No., If applicable		N.A.
9.	Nature of urgency		As per urgency Affidavit .
10	In case it is a Tax matter		N.A.
a)	Tax amount involved in the matter		
b)	Whether a reference/statement of the case was called for or rejected		N.A.
c)	Whether similar tax matters of same parties filed earlier (may be for earlier/other Assessment Year)?		N.A.
d)	Exemption Notification/Circular No		N.A.
11	Valuation of the matter		
12	Classification of the matter:		
	(Please fill up the number & name of relevant category with sub category as per the list circulated).		
	No. of Subject Category with full name		18
	No. of sub-category with full name		1807 Others
13	Title of the Act involved (Centre/State)		
a)	Sub-classification (indicate Section/Article of the Statute)		N.A.
b)	Sub-section involved		N.A.
c)	Title of the Rules involved Centre/State)		N.A.
d)	Sub-classification (indicate Rule/Sub-rule of the Statute)		N.A.
14	Point of law and question of law raised in the case		Public Records Act

15	Whether matters is not to be listed before any Hon'ble Judge?			N.A.
	Mention the name of the Hon'ble Judge			N.A.
16	Particulars of identical/similar cases, if any			N.A.
	Pending cases			N.A.
	Decided cases with citation			N.A.
17	Was S.L.P./Appeal/Writ filed against same impugned judgment/order earlier? If yes, particulars			N.A.
18	Whether the petition is against interlocutory/final order/decree in the case			N.A.
19	If it is a fresh matter, please state the name of the High Court and the Coram in the Impugned Judgment/order			N.A.
20	If the matter was already listed in this court			N.A.
a)	When was it listed?			N.A.
b)	What was the Coram?			N.A.
c)	What was the direction of the Court?			N.A.
21	Whether the date has already been fixed either by Court or on being mentioned, for the hearing of the matter? If so, please indicate the date fixed			N.A.
22	Is there a Caveator? If so, whether a notice has been issued to him			N.A.
23	Whether data entered in the Computer?			N.A.
24	If it is a criminal matter, please state			N.A.
a)	Whether accused has surrendered			N.A.
b)	Nature of Offence i.e., Convicted under section was Act			N.A.
c)	Sentence awarded			N.A.
d)	Sentence already undergone by the accused			N.A.
e)	i)	FIR/RC/Etc		N.A.
		Date of Registration of Complaint		N.A.
		Name & Place of the Police Station		N.A.
	ii)	Name & Place of Trial Court		N.A.
		Case No. in Trial Court and Date of judgment		N.A.
	iii)	Name and Place of 1st Appellate Court		NA
		Case No. in 1st Appellate Court & date of judgment –		NA

Rajeev Kumar Singh

Date: 18.06.2013 Advocate for petitioner

SYNOPSIS & LIST OF DATES

Writ Petition in Public Interest under Article 32 of the Constitution of India seeking issuance of Writ of Mandamus or any other Writ thereby directing the Respondent to take urgent steps to safeguard the Government sensitive internet communications which is "Record" as per provisions of Public Records Act and it's secrecy to be maintained as per Official Secrets Act but same is being kept outside India in US servers which is unlawfully intruded by USA Intelligence Agencies through US based internet companies under secret surveillance program called PRISM and also to ensure privacy of data of millions of Indians, under Art. 21 of the Constitution which is being unlawfully compromised by such foreign companies operating from India.

As per reports, US based nine internet companies operating in India through agreements signed with Indian users, shared 6.3 billion information/data with National Security Agency of USA without express consent of the Indian users. Such large scale spying by the USA authorities besides being against the privacy norms is also detrimental to the National Security. As per Union

Telecom Minister Mr Kapil Sibal statement, India has to build impregnable security systems to protect the networks from attacks by cyber terrorists, which has the potential to dislocate the most significant of services causing chaos and panic. However Respondent's failure to take any action against internet companies for their unlawful data sharing with USA authorities is matter of failure of implementation of Rule of Law against big and powerful internet companies.

Respondent has failed to understand the gravity of the situation and is even not aware about the details of such large scale data theft. Government communication through private internet companies leading to massive amount of proliferation and leakage of secret documents causing serious threat to security of the country. Sovereignty of Nation is on stake because no penal action being taken by the Respondent against the culprit internet companies. Such failure of Respondent in providing safety and privacy to the valued data of Indians shows the collapse of the Rule of Law which is the basic foundation of Democracy and the Constitution of India. Hence present Petition before this Hon'ble court which is custodian of Rule of Law in India.

LIST OF DATES

1993	Public Records Act enacted by Parliament which treats computer data and Emails as Records, same cannot be kept/transferred outside India without due sanction.
1995	Internet services started in India
2000	Information Technology Act passed by the Parliament wherein Sec 4 stipulates legal recognition of electronic records. So Digital agreements of internet companies with Indian users are valid enforceable contracts as per Indian Law
2007	USA National Security Agency (NSA) started project PRISM (internet data surveillance through which more than 6.3 billion data/reports of India accessed by them through internet companies) without consent of Indian users which required as per agreement

September, 2007	Internet Company Microsoft (1) joined PRISM for sharing of data with NSA
March, 2008	Internet Company Yahoo (2) joined PRISM for sharing of data with NSA
January, 2009	Internet Company Google (3) joined PRISM for sharing of data with NSA
June, 2009	Internet Company Facebook (4) joined PRISM for sharing of data with NSA
December, 2009	Internet Company PalTalk (5) joined PRISM for sharing of data with NSA
September, 2010	Internet Company YouTube (6) joined PRISM for sharing of data with NSA
February, 2011	Internet Company Skype (7) joined PRISM for sharing of data with NSA
March, 2011	Internet Company AOL (8) joined PRISM for sharing of data with NSA
October, 2012	Internet Company Apple (9) joined PRISM for sharing of data with NSA
June 7, 2013	USA secret surveillance program PRISM details leaked to media by Mr. Snowden

June 12, 2013	Government official statement shows Respondent's knee jerk reaction without any initiative to safeguard Privacy, National security and Sovereignty
June 17, 2013	Edward Snowden, who worked with National Security Agency(NSA) in the US said that technology companies claiming ignorance of the US surveillance programmes are misleading and they allowed direct access to their servers and user data to NSA
June 18 , 2013	Hence Writ Petition before this Hon'ble Court

IN THE SUPREME COURT OF INDIA

[CIVIL ORIGINAL JURISDICTION]

WRIT PETITION (C) NO. /2013

(UNDER ART. 32 OF THE CONSTITUTION)

PUBLIC INTEREST LITIGATION:

IN THE MATTER OF

PROF. S.N. SINGH

PATRON, BANAANAA.COM

A-3/45, SEC. 8, ROHNI, DELHI- 85.....PETITIONER

Versus

UNION OF INDIA

THROUGH CABINET SECRETARY ,

CABINET SECRETARIAT, RASHTRAPATI BHAWAN

NEW DELHI – 110004 ... RESPONDENT

WRIT PETITION UNDER ARTICLE 32 OF THE CONSTITUTION OF INDIA BEFORE THIS HON'BLE COURT

To,

THE HON'BLE CHIEF JUSTICE OF INDIA AND HIS COMPANION JUDGES OF THIS HON'BLE COURT

THE HUMBLE WRIT PETITION OF THE PETITIONER ABOVE NAMED

MOST RESPECTFULLY SHOWETH:

1. Writ Petition in Public Interest under Article 32 of the Constitution of India seeking issuance of Writ of Mandamus or any other Writ thereby directing the

Respondent to take urgent steps to safeguard the Government sensitive internet communications which is "Record" as per provisions of Public Records Act and it's secrecy to be maintained as per Official Secrets Act but same is being kept outside India in US servers which is unlawfully intruded by USA Intelligence Agencies through US based internet companies under secret surveillance program called PRISM and also to ensure privacy of data of millions of Indians, under Art. 21 of the Constitution which is being unlawfully compromised by such foreign companies operating from India.

As per reports, US based nine internet companies operating in India through agreements signed with Indian users, shared 6.3 billion information/data with National Security Agency of USA without express consent of the Indian users. Such large scale spying by the USA authorities besides being against the privacy norms is also detrimental to the National Security. As per Union Telecom Minister Mr Kapil Sibal statement, India has to build impregnable security systems to protect the

networks from attacks by cyber terrorists, which has the potential to dislocate the most significant of services causing chaos and panic. However Respondent's failure to take any action against internet companies for their unlawful data sharing with USA authorities is matter of failure of implementation of Rule of Law against big and powerful internet companies.

Respondent has failed to understand the gravity of the situation and is even not aware about the details of such large scale data theft. Government communication through private internet companies leading to massive amount of proliferation and leakage of secret documents causing serious threat to security of the country. Sovereignty of Nation is on stake because no penal action being taken by the Respondent against the culprit internet companies. Such failure of Respondent in providing safety and privacy to the valued data of Indians shows the collapse of the Rule of Law which is the basic foundation of Democracy and the Constitution of India. Hence present Petition before this Hon'ble court who is custodian of Rule of Law in India.

2. That, the petitioner has not approached any other concerned authority in the instant matter since the issue is of national importance and is therefore being placed before this Hon'ble court for urgent orders thereof

3. That, the petitioner herein is a citizen of India and retired as Dean of Faculty of Law, University of Delhi. Petitioner has written number of books and various articles published in Law Journals on the variety of subjects of national importance. After retirement, petitioner is associated as *Patron of Banaanaa.com, (to bring Rule of Law)* which is part of RTI Foundation initiative (Resolving to Transform India Foundation) and working towards applicability of Rule of Law in the new age areas/ subjects and also to repeal archive laws which have become redundant and thus empowering Administration of Justice in the country which is essential for inclusive growth.

4. That, the Petitioner has no personal interest in the litigation and is not guided by self-gain or for gain of any other person/institution/body and that there is no motive other than public interest and is bringing the instant issue to the attention of this Hon'ble

Court in the wider interest of people at large, that is, in bonafide public interest which is clear from the facts of the Petition.

5. That the Annexure P-1 to P-8 submitted along with the Petition are true copies of their respective originals.

6. That, no other writ petition arising out of the same cause of action has been filed by the petitioner before this Hon'ble Court, any High court or any other court.

7. That, the brief facts giving rise to the instant petition are as follows :

BRIEF FACTS-

I. That computers for the masses came to India in 1990s and Parliament passed the Public Records Act 1993 which was brought into force w.e.f. 1st March 1995 vide The Gazette of India Extraordinary (No. 119) Part II, Sec 3(ii), by which Computer data of Central Government, PSU's etc is treated as Records which cannot be sent outside India and

persons responsible for violation may be liable for punishment up-to 5 years of imprisonment.

II. That, the Internet services in India started in the year 1995 and Parliament passed the Information Technology Act, 2000. As per Sec 4 of the I.T Act provision is made for legal recognition of electronic records and hence digital agreements signed by US based internet companies with Indian Users are enforceable as per provisions of Indian Law and such companies are liable for breach of contract and infringement of privacy.

III. That the Union Government as per Sec 87 of the Information Technology Act, 2000 framed Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which provides safety measures for security of computer data which also includes Email and other communications.

IV. That, E-mails, social networking sites and E-Commerce etc. internet services are provided by various Internet Companies and most of them are registered in USA. Internet services can be accessed through mobile phones and local computer network.

As per 2012 data released by Telecom Regulatory Authority of India (TRAI), India has 929.37 million of mobile phone users and as per annual report (2012-13) of Ministry of Communication and Information Technology, approx 135 million internet service connections and India is becoming fastest growing economy for internet driven products.

V. That in the modern world of 21st Century International Relations and Defence Programs are based on Cyber Security mechanism. Most of the internet companies though doing business in India but their servers are based in USA. Such companies are entering into agreements with Indian Users and assure that data will not be shared with third parties without express consent of the users. These companies are providing following internet services to the Indian Users-

i) Emails

ii) Chat- Video Voice

iii) Videos

iv) Photos

v) VoIP

vi) File Transfer

vii) Video Conferencing

viii) Online Social- Networking

VI. That since 2007 the National Security Agency of USA has direct access to servers of internet companies to mine the user data and strategic/ sensitive files as a part of secret surveillance project PRISM. As per report, US intelligence agency NSA mined huge data from servers of following internet companies without consent of Indian Subscribers/users -

(i) Microsoft – September 2007

(ii) Yahoo - March 2008

(iii) Google – January 2009

(iv) Facebook - June 2009

(v) Pal Talk – December 2009

(vi) YouTube – September 2010

(vii) Skype - February 2011

(viii) AOL - March 2011

(ix) Apple – October 2012

A true copy of the PRISM Slides showing the details of above companies and modus operandi of such large scale surveillance operation prepared by Mr. Gaurav Pathak, Law Intern is attached as **ANNEXURE P-1** (Pages 26-31)

VII. That James R Clapper, Director of National Intelligence of USA has confirmed surveillance and acquisition of intelligence information of non-US citizens located outside the US as per the provisions of Section 702 of Foreign Intelligence Surveillance Act (FISA) . Director of National Intelligence not only confirmed the surveillance of such information but also justified that same has been used to protect USA from wide variety of threats.

A true copy of the statement by Director of National Intelligence, USA dated June 6, 2013 is attached as **ANNEXURE P-2** (Page 32-33)

VIII. That, as per reports approximately 6.3 Billion information/reports of Indian Users have been collected by US Intelligence Agencies through such internet companies under PRISM project without the knowledge or consent of Indian users. It is further reported that large number of data of

government organizations containing sensitive secret records has also been leaked to USA intelligence agencies by such internet companies.

IX. That, huge numbers of Indians are using services of above mentioned internet companies by way of emails, videos, communications etc. through digital contracts signed with such internet companies, who are under obligation to ensure the privacy of data, which cannot be shared with third parties without express consent of the Indian users.

A true copy of chart prepared on the basis of research of Ms. Pankhuri Goyal, Law Intern showing details of relevant privacy clause of such digital agreements is attached as **ANNEXURE P-3** (Page 34-35)

X. That, Public Records Act 1993 is applicable to Central Government, Union Territory , Public Sector Undertakings, Statutory bodies and Corporations and as per provisions, record includes material produced by a computer or by any other device. That as per Section 4 of the Act, no Public Records can be taken out of India without prior permission of the Government and for contravention of the

same, Sec 9 of the Act provides for punishment of imprisonment for a term of 5 years.

XI. That, as per Census of Central Govt. Employees reported by Ministry of Labor and Employment, there are approximately 30 lakh Central Government employees and majority of them use the private internet network for their email communication for official purposes. That the respondent started National Informatics Center (NIC) for intra-government email/internet communications but use of same for official purpose is not strictly complied. Thus use of private internet companies network without proper compliances, safeguards and sanction, is against law wherein data is transferred and stored at servers based in USA which is against provisions of Public Records Act and also endangering national security.

XII. That, above fact of use of private email communication is corroborated by the reports that after triple bombing in Mumbai in July 2011 terrorist attack, Prime Minister's Office issued a statement from a Hotmail address of Microsoft Corp. As per reports most of the government

departments and employees are using private internet network for important and sensitive official communications inspite of many alerts by Intelligence Bureau against such unlawful communication.

A true copy of news report stating the use of Microsoft Hotmail services by the Prime Minister Office is attached as **ANNEXURE P-4** (Pages 36-40).

XIII. That, in April 2010, hackers who were traced back to China, accessed documents from India's missile programs relating to security assessments of state's bordering China including two files which were marked as secret. As per reports, intelligence agencies issued many alerts against use of private email networks for official purposes as they may be compromising the security of the official computers and may also be causing massive amount of proliferation and leakage of secret documents causing serious threat to security and sovereignty of the country.

XIV. That, according to the FBI, terrorists are making use of the internet communication network and Cyber threats/security has become one of the prime

concern for security agencies of India since rogue activists and state sponsored agencies both are making use of the internet. It has further been confirmed by Union Telecom Minister Mr. Kapil Sibal wherein he cautioned and stated that India has to build impregnable security systems to protect the networks from attacks by cyber terrorists, which has the potential to dislocate the most significant of services causing chaos and panic.

A true copy of the Statement dated April 11, 2012 of Telecom Minister Mr. Kapil Sibal is attached as **ANNEXURE P-5** (Page 41)

XV. That, Union of India is aware of such threats which is reflected in the statement of Union Minister of State for Home Mr R.P.N. Singh before Parliament on May 7, 2013 wherein he admitted that for last 3 years more than 1000 government websites were hacked causing loss of billions of dollars to the nation. He further stated that "It has been mandated that all government websites are hosted on infrastructure of National Informatics Centre, Education and Research Network or any other

secure infrastructure service provider in the country.

A true copy of the Statement dated May 7, 2013 of the Union Minister made before Lok Sabha is attached as **ANNEXURE P-6** (Page 42-43).

XVI. That, mobile phone and internet are the two modern sources of communication and Indian security agencies are also tracking such communication for which they have to comply with Indian Laws. However, as most of the companies have their servers outside India, it has been difficult for Indian agencies to check over unlawful data/communication. Accordingly, Union of India had already issued directions to foreign telecom companies' viz. Nokia and Research in Motion (RIM – Blackberry) to establish their servers in India.

XVII. That, according to reports as per minutes of meeting home ministry has taken note of the situation and has proposed to mandate that who are operating internet telephony (VoIP) to set up their servers in India if they want to do business in India but failed to issue such directions for internet companies who are doing large scale business operations in India.

A true copy of the news report that companies doing business of VoIP will have to establish servers in India attached as **ANNEX P-7** (Pages 44-47)

XVIII. That establishment of internet companies Servers in India will not only ensure safety of Indian data from foreign intelligence agencies but also create lot of employment and economical growth through payment of various taxes which are not being paid by such internet companies for whom India is biggest market in World because China has imposed various restrictions on US companies.

XIX. That, US authorities, European Union and China government have taken cyber security issues as their top national agenda and restricted/regulated transfer of internet data outside their territory. As per reports, China has caused loss of approximately 300 billion dollars to USA companies by way of cyber hacking and misuse of IPRs and India is losing Billions of Dollars because of poor cyber security and non implementation of legal provisions. Inspite of such blatant misuse and violations by such internet companies, Government has not initiated concrete steps to get the details of 6.3

Billion information/ reports leaked to the US Intelligence agencies, which may give crucial clues about loopholes in National Security, terrorist organizations and Naxalites Movement in India.

A true copy of the PIB statement dated June 11, 2013 with knee jerk reaction of Official Spokesperson for Ministry of External Affairs is attached as **ANNEXURE P-8** (Page 48-49).

XX. That unregulated and unfettered growth of such internet companies in India without performing any legal obligation and non action of the Respondent has caused serious threat to concept of Rule of law as envisaged in article 14 of the Constitution.

XXI. That Indian economy is suffering from serious threat which is reflected in the lesser employment generation for last many years in spite of huge spending on the social sector because of diversion of most of the economic activities to internet world which is governed by Foreign Internet Companies who get all benefits without performing any obligations and compliance of Constitutional Norms and Laws of India.

XXII. That inspite of such serious reports of surveillance of Indian data by US Intelligence Agencies, government officials in India are still using the services of the aforementioned internet companies directly from their US servers against Indian Laws and thus foreign intelligence agencies have access to Indian data including the sensitive reports of Government of India, whose leakage has endangered sovereignty and security of the country.

8. That the Petitioner seeks Your Lordship's leave to prefer the instant petition under Article 32 of the Constitution of India, inter alia on the following Grounds amongst others, which are set up herein below without prejudice to each other -

GROUNDS

A. Because considering the fact that computer data/ emails are "Public Records" as mentioned in the Public Records Act, 1993 and hence such computer data/ records cannot be transferred/stored outside India.

B. Because considering the fact that disclosure of the personal/ secret information of Indian users to USA intelligence agencies is causing massive amount of

proliferation and leakage of secret documents which is causing serious threat to security and sovereignty of the country.

C. Because considering the fact that huge data of Indian government official communication is shared by internet companies with US intelligence agencies. As per provisions of Public Records Act and Official Secret Act, such companies and their CEO's are liable for penalty and prosecution.

D. Because considering the fact that such internet companies entered into agreements with Indian users with the assurance that data or information will not be disclosed or misused without express consent of the account holder but the data is getting shared with the US authorities, which is against the terms of the contract, making them liable to pay compensations for violation of Privacy.

E. Because considering the fact that digital agreement are signed as per Section 4 of the Information Technology Act, 2000 between Indian users and such internet companies which are valid legal enforceable Contract in India, hence such companies are liable for punishment under Section 43 –A and 72 -A of the Information Technology Act.

F. Because considering the fact that the Right to Privacy is Fundamental Right as per principles laid down by Hon'ble Supreme Court in PUCL Vs. Union of India, 1997 (1) SCC 301. That, US based internet companies, by disclosing the data of Indian users to US intelligence agencies without any express consent and sanction from users, have seriously dented into privacy of millions of citizens of India.

G. Because considering the fact that as per Rule 6 of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011, disclosure of sensitive data and information by a body corporate can only be done by taking prior permission from the provider of such information. However huge data of Indians had been disclosed to US Intelligence agencies by internet companies without getting the consent of the Indian users.

H. Because considering the fact that, cyber threats have surpassed terrorism in the international scenario but Respondent has failed to take effective steps for modern age challenges of Cyber security.

I. Because considering the fact that inspite of such serious reports, government officials are still using the services of such internet companies for their

official communication, making whole cyber system and national security, vulnerable in the hands of foreign intelligence agencies.

J. Because considering the fact that the respondent is duty bound to maintain records of such emails/reports so that same may be available as per provisions of Right to Information Act, 2005 but respondent has failed to do so causing serious loss to the rights of citizens of India.

K. Because considering the fact that, a large number of government officials are using services of private operators for their official communication from their personal e-mail accounts without giving details of user name and password to departmental authorities and thus violating the provisions of Public Records Act which stipulates management of such communication/records.

L. Because considering the fact that, internet companies operations in India without performing any legal obligation has caused serious threat to domestic industry and telecom companies, which are generating huge employment but not able to compete with such US based internet companies.

M. Because considering the fact that Indian economy is suffering from serious threat from such internet

companies who are not paying any taxes and operating in India in the regime of Laissez-Faire and generating huge revenue without performing any legal obligations.

N. Because considering the fact that the respondent has failed to appreciate the gravity of the situation and gross violation of privacy and also the Official Secrets Act and Public Records Act due to criminal conduct of such foreign based internet companies by becoming part of secret surveillance program of US intelligence agencies.

O. Because considering the fact that, in spite of misuse of internet communication system by the terrorists and anti-national forces, the respondent failed to initiate any concrete steps to enforce placing of servers of such companies in India which may bring uniformity and also help in effective intelligence mechanism for Indian agencies.

P. Because considering the fact that Telegraph services are coming to an end from 15 July 2013 but archive Indian Telegraph Act 1885 provisions are still being used for interpretation of modern day Mobile/internet service operations. It's ironic

that the respondent failed to enforce rules/statute on internet operations of modern world which is jeopardizing administration of justice in India.

Q. Because considering the fact that the respondent failed to check unregulated and unfettered growth of such internet companies in India who getting huge business from India but not performing any legal obligation and thus causing serious threat to concept of Rule of law as envisaged in article 14 of the constitution.

PRAYER

It is therefore respectfully prayed that this Hon'ble Court may be pleased to:

a) issue Writ of mandamus under Article 32 of the Constitution or any other appropriate writ or directions to the Respondent to prosecute CEO's of such Internet companies as per details in Para VI of the Petition, for endangering sovereignty and security of country under the provisions of Unlawful Activities (Prevention) Act 1967; and/or.

b) issue Writ of mandamus under Article 32 of the Constitution of India or any other appropriate writ or directions to respondent to initiate action against such internet companies for breach of

contract and violation of right to privacy by sharing 6.3 billion Indian data with US intelligence agencies and also to stop sharing of data with third parties without express consent of Indian users; and/or

c) issue writ of mandamus or any other appropriate writ or direction to the respondents to stop the government official communication through US based internet companies which is against provisions of Public Records Act 1993 wherein official data/records cannot be kept/transferred outside India ; and/or

d) issue writ of mandamus or any other appropriate writ or direction to the respondents to ensure that all such internet companies who are doing business in India should must establish their servers in country so that they come within Indian Tax regime and are regulated as per Indian Laws ; and/or

e) Issue writ of mandamus or any other appropriate writ or direction to the respondents to initiate disciplinary proceedings/penal action against government officials who instead of using NIC network, used private Email network of such

internet companies for official purposes without due sanction; and/ or

f) Issue writ of mandamus or any other appropriate writ or direction to the respondents to maintain email/internet communication as "Records" which may be available to Citizen of India as per provisions of Right to Information Act, 2005.

g) pass such other order/s as this Hon'ble Court may deem fit and proper.

AND FOR THIS ACT OF KINDNESS THE PETITIONER SHALL EVER PRAY

Drawn by
Virag Gupta, Advocate
Managing Partner, RTI Legal

Filed by

Rajeev Kumar Singh
Counsel for the Petitioner

Drawn on 17.06.2013
Filed on 18.06.2013

IN THE SUPREME COURT OF INDIA

[CIVIL ORIGINAL JURISDICTION]

WRIT PETITION (C) NO. /2013

PUBLIC INTEREST LITIGATION:-

IN THE MATTER OF

PROF. S.N. SINGH ...PETITIONER
PATRON BANAANAA.COM

VERSUS

UNION OF INDIA RESPONDENT

AFFIDAVIT

I, Prof. S.N. Singh, S/o Late Sh. H.P. Singh aged about 68 years R/o A-3/45, Sector 8, Rohini, Delhi - 110085 Patron of Banaaaa.com, do hereby solemnly and sincerely affirm and state on oath as under:

1. I am Petitioner in the above mentioned matter and am well acquainted with the facts and circumstances of the case, which has been drafted by my counsel under my instructions, hence competent to swear this affidavit.
2. That I have read and understood the Writ Petition Pages (1 to 24) and synopsis and list of dates in Pages (B to F) and application for interim directions (42-45) are true to the best of my knowledge and belief.
3. I say that the Annexures annexed with the Writ Petition are true/translated copies of their respective originals.

DEPONENT

VERIFICATION

Verified at New Delhi on this 18th of June, 2013, that the facts stated herein above are true and correct to my knowledge and belief, no part of it is false and nothing material has been concealed therefrom.

DEPONENT

ANNEXURE P-1

PRISM/US-984XN
Overview

OR

*The SIGAD Used **Most** in NSA Reporting*
Overview

[redacted]

April 2013

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20360901

TOP SECRET//SI//ORCON//NOFORN

TOPSECRET/SI/ORCON/NOFORN

Gmail, Facebook, MSN, Hotmail. YAHOO, Google, Apple, Skype, Paltalk, AOL mail, You Tube

Special Source Operations **PRISM/US-984XN**

PRISM

Overview

OR

The SIGAD Used **Most** in NSA Reporting

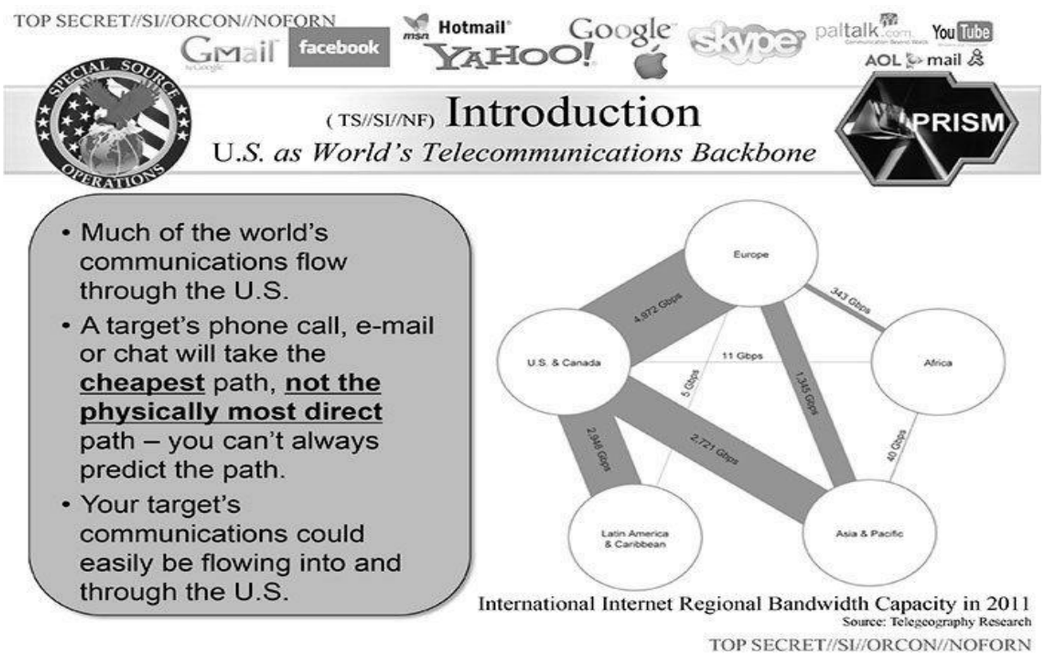
Overview

April 2013

Derived From NSA/CSSM 1-52

Dated:20070108

Declassify On 20360901



TOPSECRET/SI/ORCON/NOFORN

Gmail, Facebook, MSN, Hotmail. YAHOO, Google, Apple, Skype, Paltalk, AOL mail, You Tube

Special Source Operations (TS/SI/NF) Introduction

PRISM

U.S. as world's Telecommunications Backbone

Much of the world's communication flow through the U.S.

Europe
Africa
Asia

A target's phone call, e-mail or chat will take the cheapest path, not the physically most direct path-you can't always predict the path.

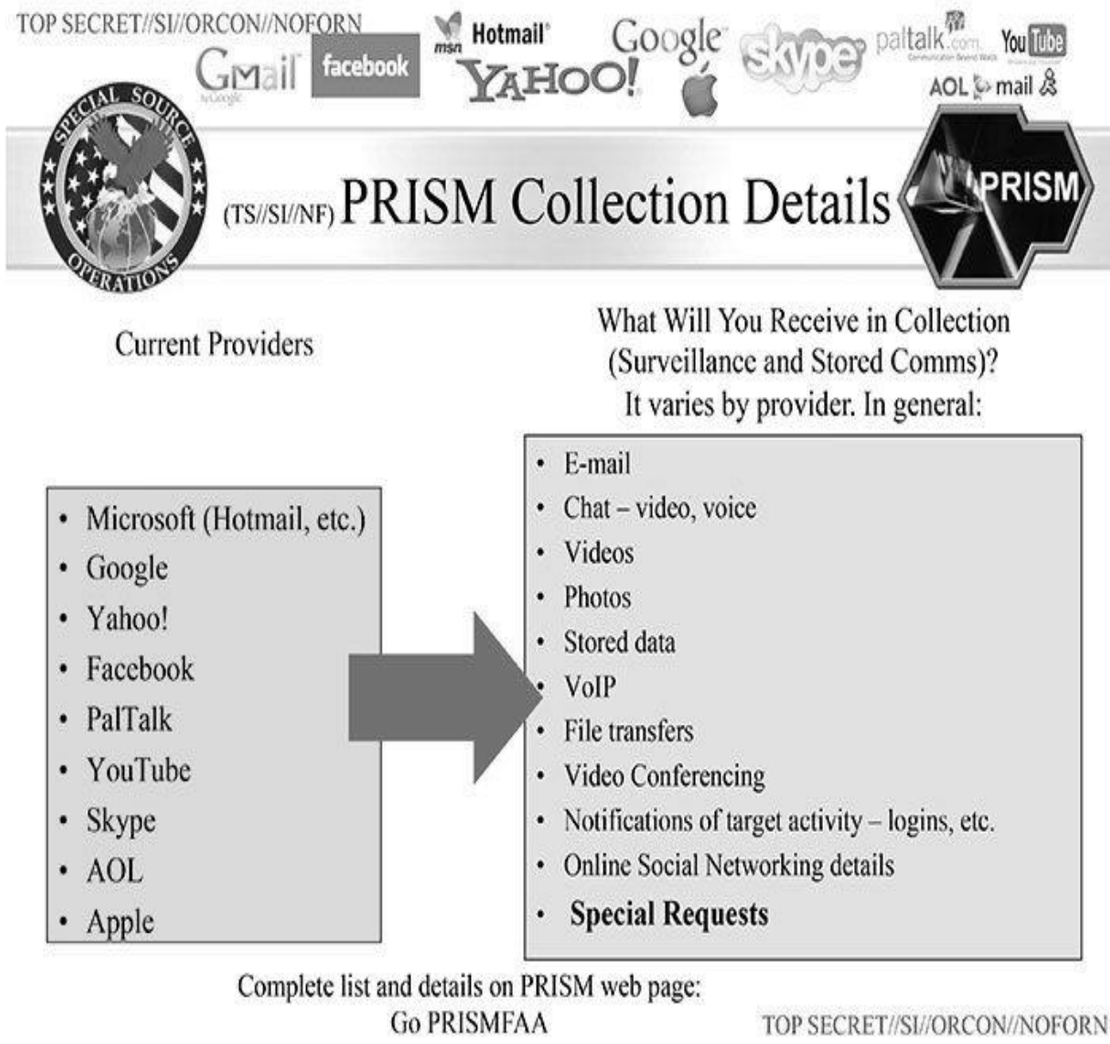
Latin America
US and Canada

International Internet Regional bandwidth capacity in 2011

Your target's communications could easily be flowing into andthrough the U.S

Source : Telegeography Research

TOPSECRET/SI/ORCON/NOFORN


TOP SECRET//SI//ORCON//NOFORN
Gmail
facebook
Hotmail
YAHOO!
Google
skype
paltalk.com
YouTube
AOL mail
SPECIAL SOURCE OPERATIONS
(TS//SI//NF) PRISM Collection Details
PRISM
Current Providers
What Will You Receive in Collection (Surveillance and Stored Comms)? It varies by provider. In general:
• Microsoft (Hotmail, etc.)
• Google
• Yahoo!
• Facebook
• PalTalk
• YouTube
• Skype
• AOL
• Apple
• E-mail
• Chat – video, voice
• Videos
• Photos
• Stored data
• VoIP
• File transfers
• Video Conferencing
• Notifications of target activity – logins, etc.
• Online Social Networking details
• Special Requests
Complete list and details on PRISM web page:
Go PRISMFAA
TOP SECRET//SI//ORCON//NOFORN

Gmail, Facebook, MSN, Hotmail. YAHOO, Google, Apple, Skype, Paltalk, AOL mail, You Tube

Special Source Operations (TS/SI/NF) PRISM

PRISM Collection Details

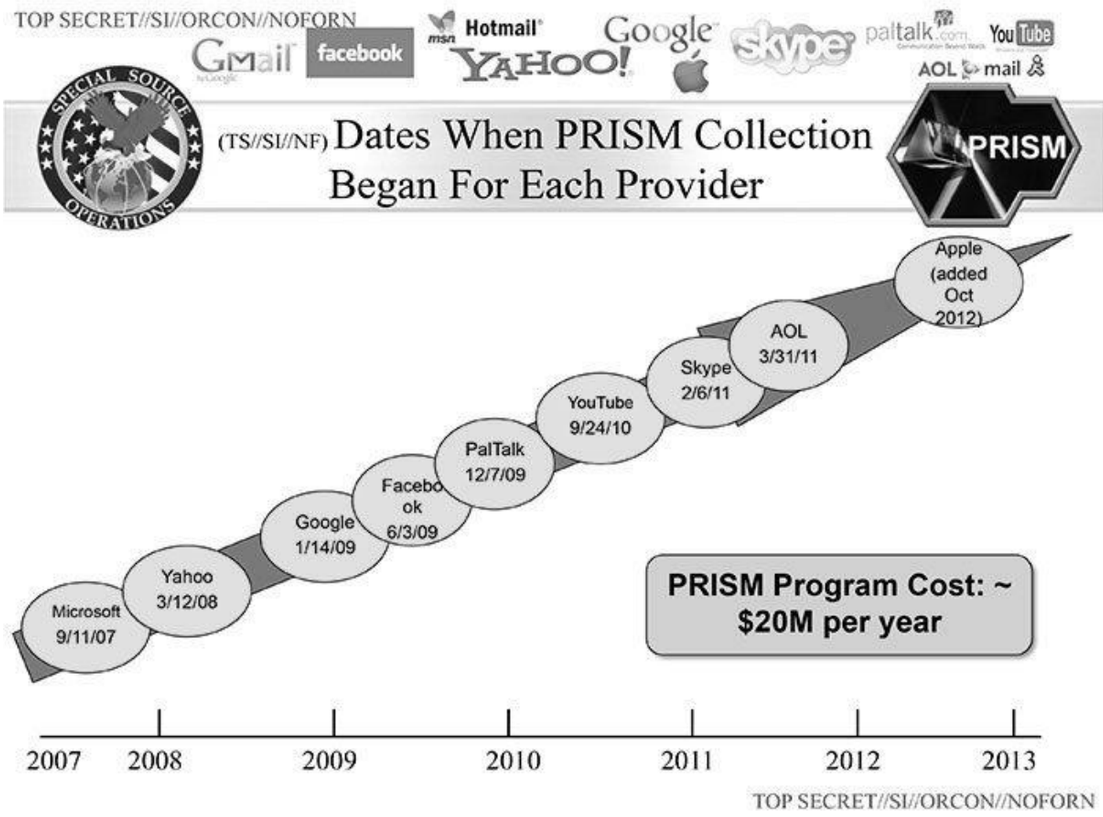
Current Providers	What will You Receive in Collection (Surveillance and Stored Comms)? It varies by provider. In general:
Microsoft (Hotmail,etc.)	E-mail
Google	Chat-video, voice
Yahoo!	Videos
Facebook	Photos
PalTalk	Stored Data
Youtube	VoIP
Skype	File Transfer
AOL	Video Conferencing
Apple	Notifications of target activity – logins,
	Online Social Networking Details
	Special Requests

Complete list and details on PRISM web page:
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN

Complied by Mr. Gaurav Pathak – Law Intern

IV Semester B.A. LL.B. (Hons.), Dr. RML National Law University, Lucknow

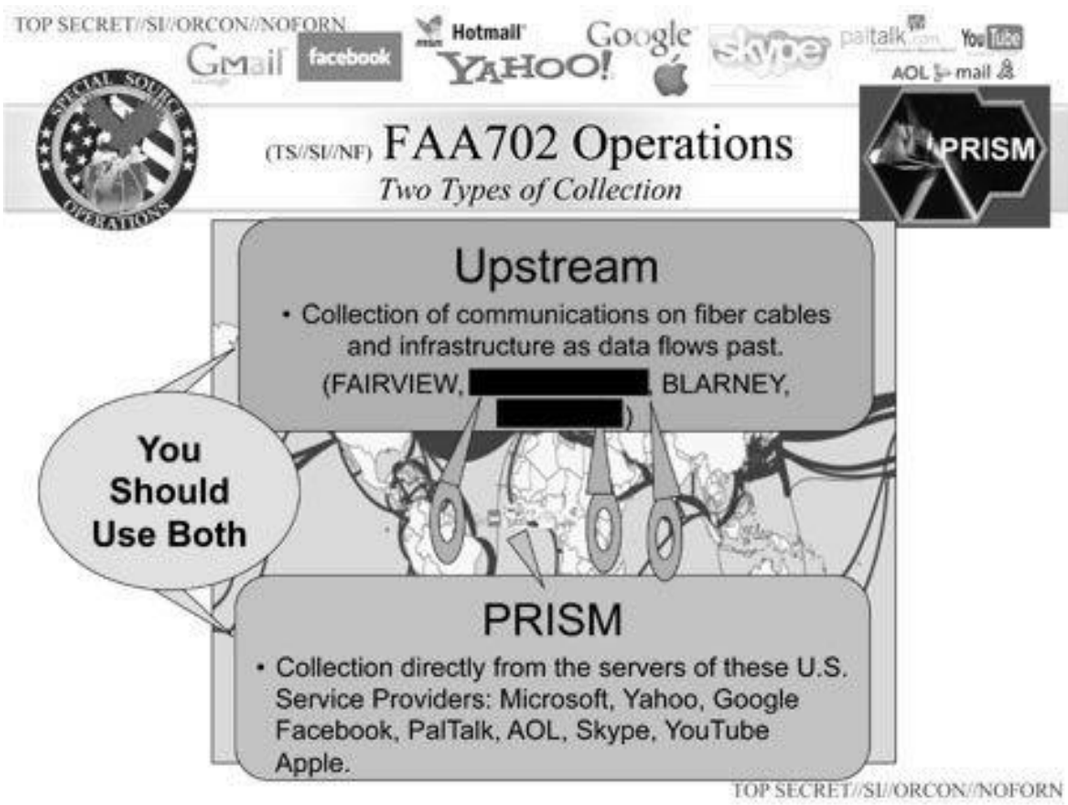


TOPSECRET/SI/ORCON/NOFORN

Gmail, Facebook, MSN, Hotmail. YAHOO, Google, Apple, Skype, Paltalk, AOL mail, You Tube

PRISM

Dates When PRISM Collection Began For Each Provider
(TS//SI//NF)
Microsoft – 9/11/07
Yahoo – 3/12/08
Google – 1/14/09
Facebook – 6/3/09
Paltalk – 12/7/09
Youtube – 9/24//10
Skype – 2/6/11
AOL – 3/31/11
Apple – Oct 2012
PRISM Program Cost: - $20M per annum



TOP SECRET//SI//ORCON//NOFORN

Gmail , Facebook, Hotmail, Yahoo, Google, Apple, Skype, Pal Talk, Youtube, AOL

(TS//SI//NF) FAA702Operations

Two types of Collection (You should use both)

- Upstream- Collection of Communication on fiber cables and infrastructure as data flows past.(FAIRVIEW, BLARNEY)
- PRISM- Collection directly from the servers of these US service providers: Microsoft, Yahoo, Google, Facebook, Pal talk, AOL Skype, Youtube, Apple.

  TOP SECRET//SI//ORCON//NOFORN

//True Copy//

ANNEXURE P-2

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

DNI Statement on Activities Authorized Under Section 702 of FISA

June 6, 2013

The Guardian and *The Washington Post* articles refer to collection of communications pursuant to Section 702 of the Foreign Intelligence Surveillance Act. They contain numerous inaccuracies.

Section 702 is a provision of FISA that is designed to facilitate the acquisition of foreign intelligence information concerning non-U.S. persons located outside the United States. It cannot be used to intentionally target any U.S. citizen, any other U.S. person, or anyone located within the United States.

Activities authorized by Section 702 are subject to oversight by the Foreign Intelligence Surveillance Court, the Executive Branch, and Congress. They involve extensive procedures, specifically approved by the court, to ensure that only non-U.S. persons outside the U.S. are targeted, and that minimize the acquisition, retention and dissemination of incidentally acquired information about U.S. persons.

Section 702 was recently reauthorized by Congress after extensive hearings and debate. Information collected under this program is among the most important and valuable foreign intelligence information we collect, and is used to protect our nation from a wide variety of threats.

The unauthorized disclosure of information about this important and entirely legal program is reprehensible and risks important protections for the security of Americans.

James R. Clapper, Director of National Intelligence

//True Copy//

ANNEXURE P-3

Relevant Clauses of Privacy Policy

Yahoo

Yahoo! does not rent, sell , or share personal information about you with other people or non-affiliated companies except to provide products or services you've requested, when we have your permission..

We transfer information about you if Yahoo! is acquired by or merged with another company. In this event, Yahoo! will notify you before information about you is transferred and becomes subject to a different privacy policy.

Google and YouTube

With Your Consent

We will share personal information with companies, organizations or individuals outside of Google when we have your consent to do so. We require opt-in consent for the sharing of any sensitive personal information.

Facebook

How we use the information we receive

While you are allowing us to use the information we receive about you, you always own all of your information. You trust is important to us, which is why we don't share information we receive about you with others unless we have:

- Received your permission;
- Given you notice, such as telling you about it in this policy; or
- Removed your name or any other personally identified information from it.

Complied by Ms. Pankhuri Goyal – Law Intern

II Semester, Amity University, Jaipur

//True Copy//

ANNEXURE P-4

Bloomberg Business week

India Government's Use of Hotmail, Gmail 'Recipe for Disaster'

By Mehul Srivastava on July 18, 2011

July 19 (Bloomberg) After a triple bombing in Mumbai killed 21 people last week, Prime Minister Manmohan Singh's office issued a statement condemning the terrorist attacks -- from a Microsoft Corp. Hotmail address. Singh's staff's use of a free e-mail account is typical of most government workers, who log into Hotmail, Google Inc.'s Gmail and Yahoo! Inc.'s e-mail to conduct official business. They also list those addresses on agency websites and business cards. Bureaucrats avoid the government system because it covers only 10 percent of federal employees, don't include the latest security patches and can't be accessed via India's 840 million mobile-phone connections.

That preference for free e-mail accounts threatens the safety and veracity of government information because the data is moving through computer servers outside India, cyber security experts said. "It's a recipe for disaster," said Pawan Duggal, a New Delhi lawyer who argues information-technology cases before India's Supreme

Court. “It’s really quite amazing that, as a nation, we haven’t yet woken up to the idea that sensitive government information should be shared through secure channels, not Hotmail or Yahoo.” Tata Consultancy, Infosys The Ministry of Commerce sends market-moving inflation data via a Gmail account, and the Indian Air Force uses another to send media updates on competitive bidding for an $11 billion combat-jet program.

After a July 6 interview with Bloomberg News, Attorney General Goolam Vahanvati handed out Hotmail and Gmail addresses as the best ways to contact him. Public servants shun an e-mail system in a nation with an $88.1 billion IT industry employing 2.5 million workers, making India the world’s largest outsourcing destination. The nation’s three biggest IT companies - Tata Consultancy Services Ltd., Infosys Ltd. and Wipro Ltd. count Deutsche Bank AG and Citigroup Inc. among their clients. The government system created by the New Delhi-based National Informatics Center usually requires an Internet- connected computer, and the World Bank said last year that fewer than 5 percent of Indians have ever used the Internet. Indians typically use smartphones to access e-mail. Only senior government officials have smartphone access to federal e-mail, and a security precaution prevents them from sending messages to other NIC addresses, according to the NIC website. Hacking Worries B. K.

Gairola, the director general of the NIC, did not respond to several phone calls and an e-mail seeking comment.

"It certainly makes sense that lots of people around India use Hotmail for all sorts of e-mail, both official and personal," Microsoft's India unit said in an e-mail. "Hotmail is convenient, secure and easily accessible." Google's Gurgaon-based spokeswoman, Paroma Chowdhury, declined to comment. A week before the terrorist attacks, Singh's office used Hotmail to send condolences to the families of 65 people killed in a train derailment. 'Alarming' Situation Singh's spokesman, Harish Khare, did not respond to an e- mail sent to his government account seeking comment. Using the government system requires going through NIC's website. During the past decade, NIC created about 300,000 e- mail accounts for India's 3.1 million federal employees to access through secure servers, said Siba Charan Pradhan, who is in charge of the messaging systems and anti-virus unit at NIC.

India's domestic Intelligence Bureau issued a directive saying government workers must use official e-mail accounts, Pradhan said. Accessing NIC's website is complicated for those in remote parts of India, where Internet access is spotty and slow. Ministry of Environment and Forests employees list their Hotmail and Gmail addresses on the website because even basic mobile phones can

receive e-mails, said Eknath Muley, a former director who retired last year. “It’s quite alarming and sad that this is the situation in a country where the private sector IT companies are so advanced,” said Rakshit Tandon, a consultant with the Internet and Mobile Association of India, an industry group. “The use of private e-mail accounts needs to be stopped, once and for all.”

Veracity Questioned The government also is creating potential legal troubles for itself by using Hotmail and Gmail accounts, Duggal said. The host servers often are outside India, making jurisdiction complicated during instances of cyber fraud or hacking. The Supreme Court has said in several cases that it doesn’t trust government statements or data sent through a free e-mail account, so it requested information through official accounts instead.“When an official is defending himself by presenting information or exchanges from a free account, it produces the question of authenticity and veracity of information,” Duggal said. “And that starts giving the opposite end the opportunity to stand and challenge it.” E-Mail ‘Leakage’. Before the government depends on its own e mails, the system has to be upgraded to fix flaws, and users have to be taught to be more sophisticated, Tandon said.

Official websites often don’t have the latest security patches, and employees share or use common passwords. “There is a massive

amount of proliferation and leakage in the government sector," said Tandon, whose group has held workshops on cyber security with about 5,000 government officials. The website of the Central Bureau of Investigation, India's equivalent of the FBI, was defaced with anti-Indian messages in December.

The government denied July 6 reports in local media that the website for the National Security Guards, the elite counter-terrorism unit, had been hacked .In April 2010, hackers traced back to China accessed documents from India's missile programs, security assessments of states bordering China and files from embassies worldwide, including two marked "secret," according to a report by Information Warfare Monitor, a research group associated with the University of Toronto. The Indian government was unaware of the attack until informed by researchers, the group said. --Editors: Michael Tighe, Bret Okeson.

//True Copy//

ANNEUXRE P-5

THE HINDU

Sibal: beware of cyber terrorists

April 11, 2012

Minister for Communications Kapil Sibal has said that while a lot of work needs to be done by industry to make high-tech telecom services affordable to the aam admi, there was a pressing need to protect the networks from cyber terrorists. “As society becomes more connected, we have to build impregnable security systems to protect the networks from attacks by cyber terrorists, which has the potential to dislocate the most significant of services causing chaos and panic.

In the absence of adequate security, we will be exposing ourselves to disaster,” Mr. Sibal warned. He was in the city to launch the country's first 4G service.

“Wars of tomorrow”

“The wars of tomorrow will not be fought by men in battlefields. The wars of tomorrow will be through cyber attacks,” he said. “We have to be careful.” He appealed to all sections of industry and entrepreneurs to ensure that security was an integral part of a network.

//True Copy//

ANNNEUXRE P-6

THE TIMES OF INDIA

Over 1,000 government websites hacked in last 3 years

PTI May 7, 2013,

NEW DELHI : More than 1 ,000 government websites belonging to various ministries and departments were hacked in the last three years.

Minister of State for Home RPN Singh today said as per information reported to and tracked by Indian Computer Emergency Response Team (CERT-I n), a total of 303, 308 , 371 and 48 government websites belonging to various Ministries and Departments were hacked during 2010, 2011 , 2012 and up to March 2013, respectively .

"Department of Information Technology has taken necessary preventive actions to hacking of the government websites/sensitive data," he said in a written reply in Lok Sabha.

Singh said the preventive action includes proper audit of all new government websites and applications in respect of cyber security prior to their hosting.

"It has been mandated that all government websites are hosted on infrastructure of National Informatics Centre, Education and

Research Network or any other secure infrastructure service provider in the country ," he said.

//True Copy//

ANNEXURE P-7

THE TIMES OF INDIA

Government wants Skype to set up servers in India

Joji Thomas Philip, ET Bureau May 20, 2013,

NEW DELHI: India may ask all firms offering internet telephony, including popular online phone service provider Skype, to set up servers in the country if they want to continue offering this facility here. The move is aimed at allowing law enforcement and security agencies get access to newer forms of communications that cannot be tracked by traditional monitoring systems. The Centre has also decided to ask internet service providers and mobile phone companies to 'segregate Internet Protocol (IP) addresses on a state basis', a step that will allow the government to block social networking sites or any other websites and even internet telephony on select states or regions in the country.

These decisions were taken in a home ministry meeting on April 23 that was attended by representatives from Intelligence Bureau, other security agencies, top police forces and senior officials from telecom and IT departments. ET had reviewed the minutes of this meeting. "Any service provider, who provides communication service in India via any media through Voice-over-Internet Protocol (VoIP), should be mandated to be registered in India, having its office, server located in

the country and therefore, subject to Indian laws. Necessary provisions to this effect may be incorporated through amendment in Indian Telegraph Act, 1885 and Information Technology Act, 2000," the minutes of the meeting said.

This solution was proposed after both the telecom and IT departments said it would be not possible to intercept internet telephony communications on a regional basis, or even block these in specific states and regions, due to 'unregulated internet architecture in India and highly decentralised encrypted structure of Skype'. The minutes of the April 23 meeting also add that segregating IP addresses on a regional basis will 'facilitate home secretaries to allow lawful interception in areas under their jurisdiction under the Indian Telegraph Act and Information Technology Act'.

According to international media reports, Microsoft-owned Skype, which has been popular with those who did not want their communications to be tracked by governments, had last year made technical upgrades and also expanded cooperation with law enforcement authorities. India has been pushing IT majors and even handset companies to set up servers here resulting in the likes of BlackBerry and Nokia setting up interception facilities here to help intelligence agencies monitor communications on these devices. At the same time, the telecom department's research body C-DOT has also begun installing indigenously developed monitoring solutions on

the networks of internet service providers (ISPs) and telcos. During the April 23 meeting, it was also decided that all 'ISPs and telcos must designate a nodal officer in each state with access to GGSN gateway.

In common parlance, the nodal officer must have access to that part of the network that is responsible for the delivery of data packets from and to the mobile stations within a geographical service area."The telecom department will also ensure that each state will have facilities for lawful interception of internet," the minutes add. India has been seeking to arm itself with the technological capabilities to block Twitter and other social networking sites in select states and regions after the government failed in its attempts last year to shut down social media in some parts of the country. The government’s efforts had failed after telcos refused to comply stating that they lacked the technology to bar websites on a state-by-state basis.

On August 23 last year, the home ministry had asked the information technology ministry to direct ISPs and telcos to block Twitter in eight states â€” Kerala, Assam, Tamil Nadu, Andhra Pradesh, Maharashtra, Karnataka, Gujarat and Uttar Pradesh â€” amid concerns that the popular social networking website was being used to fan communal tensions following violence in Bodo-dominated areas of Assam. But the Twitter ban order could not be implemented after telcos said they could only block websites and social networking sites on a national

basis. Following this, in an August 27 meeting in the Prime Minister's Office, which was attended by heads of all intelligence agencies as well as representatives from the ministries of home, telecom and IT, the government decided to set up an 'appropriate regime' to address issues related to blocking content on the internet and social media in a 'smart, timely and consistent manner'. The new regime was to work out an effective cyber monitoring system, lay out guidelines and operating procedures on the nature of online content that would be blocked and also specify penalties for perpetrators.

//True Copy//

ANNEXURE P-8

Transcript of Media briefing by Official Spokesperson
June 11, 2013

Official Spokesperson (Shri Syed Akbaruddin): Good afternoon friends and thank you very much for being here this afternoon. Since we had not met for quite some time in this format I thought it would be useful to have our usual interaction. As usual, I will begin with an announcement that I have to make following which you are free to ask me questions on that first and subsequently on anything else that you would like.

Official Spokesperson: If you want to ask whether we are concerned by media disclosures suggesting that data relating to private communications of Indian citizens may have been harvested, my answer to you is, yes we are concerned and surprised about it. Between India and the US we have a Cyber Security Dialogue, and it is coordinated by the National Security Councils on both the sides. We feel that this is the appropriate forum to discuss such issues. We intend to seek information and details during consultations between interlocutors from both sides on this matter in that appropriate forum.

If you ask that if it is discovered that Indian laws relating to privacy of information have been violated what would be the view of the Indian Government, obviously we would find it unacceptable. If Indian laws

relating to privacy of information of ordinary Indian citizens have been violated, surely we would find it unacceptable. I hope broadly I have tried to respond to you on where we stand.

Of course, this is an evolving situation. Every day we find new issues coming up. Rather than jump to conclusions at this stage, we will take it as it evolves and have a better understanding and a clearer paradigm of how to tackle this issue once the broader parameters of this in its entirety are available for us.

//True Copy//

IN THE SUPREME COURT OF INDIA

[CIVIL ORIGINAL JURISDICTION]

I.A. No...../2013

IN

WRIT PETITION (C) NO. /2013

IN THE MATTER OF:-

PROF. S.N. SINGH ...PETITIONER

PATRON, BANAANAA.COM

VERSUS

UNION OF INDIA ...RESPONDENT

APPLICATION FOR AD- INTERIM DIRECTIONS

To,

THE HON'BLE CHIEF JUSTICE OF INDIA AND HIS COMPANION JUDGES OF THIS HON'BLE COURT

THE HUMBLE WRIT PETITION OF THE PETITIONER ABOVE NAMED

MOST RESPECTFULLY SHOWETH:

1. That the petitioner is a Citizen of India and is approaching this Hon'ble Court under Article 32 of the Constitution of India for issuance of writ of mandamus or any other writ thereby directing the respondents as per prayer detailed in accompanying writ petition.

2. Petitioner has sought directions to take urgent steps to safeguard the Government sensitive internet communications which is "Record" as per provisions of Public Records Act and secrecy to be maintained as per Official Secrets Act but same being

unlawfully kept outside India in USA servers which is intruded by USA Intelligence Agencies through US based internet companies under secret surveillance program called PRISM and also to ensure privacy of data of millions of Indians, under Art. 21 of the Constitution which is unlawfully compromised by such foreign companies operating from India.

3. That the Respondent failed to check unregulated and unfettered growth of such internet companies in India which are getting huge business from India but not performing any legal obligation and thus causing serious threat to concept of Rule of law as envisaged in article 14 of the constitution

4. That the petitioner has stated the facts of the case and the grounds arising therefrom in the accompanying petition and the same may be treated as part and parcel of the present application, and the same is not being reproduced herein for the sake of brevity.

PRAYER

It is therefore most respectfully prayed that this Hon'ble Court may be pleased to issue ad- interim directions to the Respondent

a) That the Government Officials should be restrained from using the services of such private internet companies for official communication as the data/records is being stored in Foreign country which tracked by US intelligence agencies without any authority which endangering sovereignty and integrity of country; and/ or

b) That the respondent be directed to get the details of information/records which has been shared by such internet companies with foreign intelligence agencies so that they can be sued and prosecuted for violation of privacy laws.

c) That the respondent be directed to take concrete steps to immediately stop the sharing of data by internet companies with foreign intelligence agencies without express consent of Indian users.

d) Pass such other order/orders as this Hon'ble Court may deem fit and proper.

AND FOR THIS ACT OF KINDNESS THE PETITIONER SHALL EVER PRAY

Drawn by
Virag Gupta, Advocate
Drawn on 15.06.2013
Filed on 18.06.2013

Filed by

Rajeev Kumar Singh
Counsel for the Petitioner