



**Shashanka
Shekhar Panda**

SADF FOCUS

Why A Cyberterrorism Focused ‘Data Governance Policy’ Would Win in India Where a “Draft National Encryption Policy” Could Not

Abstract

Data Governance is a major area of concern globally. It evokes sharp reactions and divides nation along sharp fault lines. The stakes are high for businesses, for citizens and governments, all alike.

A few days ago, the Indian government published its Draft National Encryption Policy. The badly written draft met with stiff public and political resistance. The emergent public resistance driven by lack of conceptual knowledge except in very informed circles leading to fear of big government snooping on citizens and the spiralling media frenzy led the government to withdraw the well-intentioned, albeit technically flawed, draft.

Hereunder, I discuss the flaws of the policy that led to its early demise, the focus that the draft should have had, the underlying exigent national security imperatives, trade-off between the sovereignty of India and the individual freedom of Indians and the policy options ahead of the government to device a cogent data governance policy in India.

[South Asia Democratic Forum \(SADF\)](#)

19 Avenue des Arts 2nd
floor, 1210 Brussels,
Belgium

info@sadf.eu
www.sadf.eu

+12 026 834 180;
+32 2 808 42 08

Reg. Num. BE 833606320

Keywords: Cyberterrorism, Cyber Security, India, Draft National Encryption Policy, Data governance

A Stellar Wind

A few days ago, a data-scientist colleague of mine and I were indulging in a conversation on data governance. The conversation traversed very quickly into the realm of cyberterrorism especially in the context of “Stellar Wind”, a sort of a euphemistically eponymous codename given to the President’s Surveillance Program in the United States of America. Taking that as the backdrop, we were discussing the various aspects – technological, legal, political and ethical.

It stands to reason that the name “Stellar Wind” has been derived from an identical term in Astrophysics that refers to the flow of gas from the upper atmosphere of a star system. As a direct corollary, pollinated into the world of cyber intelligence, it would loosely mean a mechanism to monitor otherwise unreachable flow of personal, encrypted information generated by the universe of Internet users.

Hot on the heels of this discussion, on September 21, 2015, the Department of Information Technology of the Government of India released the Draft National Encryption Policy (“Draft”, hereinafter). Thereby hangs a tale that was to end very quickly in the summary withdrawal of the Draft, consequent upon the hue and cry over privacy-invasion issues.

However in matters of public policy, especially one that impacts the world of internet technologies and the footprint of digital data, it’s rather simplistic to assume that with the extinguishment of the draft policy the last word has been said and heard on this burning issue. The geostrategic realities of the borderless cyberworld are bound to fan the fires of data governance soon in foreseeable future. It’s up to the Narendra Modi government to react to it or respond pre-emptively. The Minister of State for Information Technology Mr Ravi Shankar Prasad has assured us that they would soon issue a reworked draft.

Devils In The Draft

One reading of the draft and you knew what was wrong with it. The draft started by introducing us to the importance of encryption and cryptography. It then asserted, both in part II and III, viz., the Mission and the Vision respectively, the centrality of a secure environment for the transaction of information in cyberspace. In part IV, viz., the Objectives, it specified the use of encryption for ensuring confidentiality and the protection of privacy as the primary goals. In effect it consistently established the principle of a strong data encryption regime as the bedrock of the draft.;so far so good.

Here’s where things went downhill. In the next part, i.e. part IV, viz., Strategies, that became the bone of contention, the policy mentioned steps, that would in-effect, in the eyes of the citizens, academia, civil society, especially civil liberties group, the political opposition particularly the Left Liberals, take apart any meaningful regime of data encryption for millions of users of internet in India and instead expose them to hackers exploiting easy vulnerabilities.

The policy suggested that users in the B2B (business to business) and the B2C (business to citizens) sectors shall reproduce, “on demand”, the plain and encrypted text pairs of the information transacted. It went on to say that such record should have to be kept for a period of 90 days from the date of the transaction. The draft collapsed under the weight of its own inherent contradictions.

The din over privacy issues acted as a catalyst and a perfect political storm was in the offing. Significant damage to the perception of the government was avoided as Ravi Shankar Prasad acted swiftly and the draft was consequently recalled but not before the Indian media went to town with it and the political opposition parties seized the moment in launching a broadside against the Narendra Modi government, calling the draft an attack on the freedom of the people.

Breaking The Draft Code: Blueprint To Avoiding Future Lapses

The draft’s stated strategies in substance would have effectually decrypted the data, thereby exposing it to theft by the most plebeian of hackers and likely by even malware crawling on the internet. In doing so it would have contradicted the big talk of the mission, vision and the hallowed objectives of attaining data integrity. Whatever else the objectives might have been, it most certainly was not even in the remote vicinity of ensuring data encryption, because it did just the opposite.

Much as the political opposition would love to call this a direct frontal attack on privacy, it would be touch naïve to assume that any government, in such plain sight, would make a brazen attempt to lay down rules to steal data for political use and then discuss those with the public, inviting wide consultations on the draft policy and that too in what would definitely be the most roundabout and perhaps ineffectual way of going about doing it! If ever such a plan is at all executed, it is likely to be done clandestinely, by stealth and not with such level of transparency, which would render the operation a farce. Point is, the good intentions of Narendra Modi government don’t seem to be in doubt. Unless one really thinks that Narendra Modi is stupid. He has been called a lot of things, but stupid is certainly not one of them.

So, then, what was the objective? Those who are informed of the global context of the debate of data governance would not lose much time before figuring out the answer. Hint: if you read the opening paragraph of this article, it would dawn on the readers that data experts, cyber security experts and those grappling with the ethical fallouts of data integrity, encryption and privacy would have already been expecting, nay, demanding initiation of a policy discourse on the burning issue of data governance.

Bugs In The Draft Data Encryption Policy

First, the draft should not have had the narrow perspective that it did have and therefore should never have been called a Draft National Encryption Policy to begin with. It should have addressed a broader and a more serious series of data governance challenges. The primary challenge should have been that of Cyberterrorism and it should have clearly elaborated on the nature, extent and the seriousness of the threat, giving a global context. It should therefore have been given a more

comprehensive name, simply the Draft Data Governance Policy. Only by taking such a holistic viewpoint could justice have been done to the policy. The draft failed because of its flawed tunnel vision.

The draft should have mentioned the national security imperatives upfront, specifically cyberterrorism. It never did and the word “cyberterrorism” never appears in it. It should cited cyberterrorism as the single most important factor by far, that ordains and dictates the launch a full scale, systemic, knowledge capital based, research and development led, technological counteroffensive and policy driven cyber intelligence institution.

Secondly, technologically, the draft lends itself to dabbling in superficial half measures. Instead of creating a fool proof system, it puts the onus on users to maintain a 90-day record of plain text and encrypted text pairs of all information transactions.

Purely within the ambit of the draft policy, predicating the efficacy of a counter cyberterrorism, i.e. cyber intelligence effort on the predilections of the user, who might also turn out to be a hostile or rogue element, upon the suspected event of an act of cyberterrorism actually devolving, which should and would also be the natural premise of any such counter cyberterrorism operation to start with anyway, as the systemic key to the entire technological framework, is the most absurdist architecture imaginable.

Not to mention the fact that in those 99% cases where the user is likely to be innocuous, the probability that the user would be even aware of the existence of such terms as “encryption”, “cryptography”, “hash”, “key”, “public key” is bleak and should be assumed to be an impossibility. A technological system driven on something as complex as programming codes that are supposed to be geared up to tracking anti national activities such as cyberterrorism in real time is bound to collapse if it depends on human intervention, that too at the targeted end, for maintaining its integrity. This is laughable and hilarious to say the least. As my data scientist friend and colleague said – “people don’t even understand the difference between “http” and “https” yet”. Actually! And why the hell should they bother?

Data Governance And Cyberterrorism: Setting Priorities

Data governance needs to be seen most urgently and most necessarily in the context of cyberterrorism. cyberterrorism is a recent face of asymmetric warfare which is very competently deployed to devastating effect by organized gangs of terrorists, such as ISIS. cyberterrorism today is one of the biggest threats to the sovereignty of nations and a very effective tool in organizing and coordinating recruitment of disgruntled elements, launching funding efforts, spreading a campaign of hatred and plotting terror attacks.

Very importantly focus on cyberterrorism would evoke empathy and a far critical attitude from citizens. Let’s again look at the progression of “Stellar Wind”. There was resistance to the surveillance program both within government and from the public. Anti-snooping heroes of the world such as the Edward Snowden, Julian Assange et al have railed against the efforts of

governments to snoop on citizens, building up massive public opinion against government. Yet, Stellar Wind is here to stay because the threat to sovereignty from the enemy, as just discussed, is simply too grave to be ignored and sacrificed at the altar of individual privacy.

cyberterrorism is the scourge that needs to be fought with Data Governance technologies, systems, mechanisms that defer to the asymmetric nature of the technique that uses such fancy and mostly unheard of methods as Steganography to spread the tentacles of terror. cyberterrorism is the leverage that allows lone wolves and to acquire dangerous proportions. Recall the infamous case of @ShamiWitness, the Twitter handle of a Muslim youth from the cybercity of Hyderabad, India. He was suspected to be running a successful and elaborate recruitment and organizing ring on Twitter on his laptop for ISIS. He was tracked and finally caught by India's intelligence agencies in December 2014, post advent of the Narendra Modi government and Ajit Doval as the National Security Advisor to Prime Minister Narendra Modi. Considering a rudimentary cyber-intelligence operation, this is suspected to be a snowflake on the tip of the iceberg.

Hence, the discourse on Data Governance must start with an order of precedence to priorities. Privacy and freedom of citizens is very important. But the discourse cannot end there. Privacy and freedom are meaningful only when the sovereignty of the nation, the integrity of the motherland stays intact. cyberterrorism is both a weaponizing mechanism and a weapon itself, threatening the integrity and sovereignty of India, putting India on a dangerous course to conflicts and strife.

The stated policy must put the need to save us from the threat of cyberterrorism at a higher order than the need to protect our privacy and freedom. The Primary Objective must be – Secure Sovereignty. If individual privacy and freedom, however exalted an idea they might be in a democracy, be in conflict with prevention of an event of cyberterrorism, which is deemed to be an attack on the sovereignty of the nation, the latter must gain precedence.

The Empire Strikes Back: Cyber Intelligence Counterstrike

Thus, having established the first principle of the order of precedence of objectives, we must understand how best we can technologically deal with the challenge. Let's go back to Stellar Wind again, the most formidable system of cyber intelligence known to man. Stellar Wind works like a vacuum pump of astronomical proportions. It is suspected to suck data from around the globe at the rate of yottaflop (10^{24}) operations per seconds. This data is not just in the shape of Internet digital data but also in the shape of cellular conversations from around the world. How's it able to get access to so much data at a pan global scale?

It's able to do that because of the direct or extended jurisdiction the government of United States has over computer servers, communication satellites, underground and undersea communication cables that might be owned by the biggest names in the world of technology and are housed in USA domestically or over which USA has legal jurisdiction. Stellar Wind also goes beyond just ordinary

private data capture. It employs supercomputers that are suspected to be close to cracking Advanced Encryption Standard (AES) level 256 bit encryption algorithms.

"A project of immense secrecy, it is the final piece in a complex puzzle assembled over the past decade. Its purpose: to intercept, decipher, analyze, and store vast swaths of the world's communications as they zap down from satellites and zip through the underground and undersea cables of international, foreign, and domestic networks. The heavily fortified \$2 billion center should be up and running in September 2013. Flowing through its servers and routers and stored in near bottomless databases will be all forms of communication, including the complete contents of private emails, cell phone calls, and Google searches, as well as all sorts of personal data trails—parking receipts, travel itineraries, bookstore purchases, and other digital "pocket litter." It is, in some measure, the realization of the "total information awareness" program created during the first term of the Bush administration—an effort that was killed by Congress in 2003 after it caused an outcry over its potential for invading Americans' privacy."

James Bamford on "Stellar Wind", The NSA is building the Country's Biggest Spy Center in "Wired", March 15, 2012

The discourse in India, as evidenced in the draft, is nowhere remotely close to building a Stellar Wind. Also, it need not be the endeavor to mimic Stellar Wind, in toto. The strategy stated in the withdrawn draft was beset with multiple ills, talking from a pure technological perspective. The draft was very narrow and constricted in its approach and offers very crude, sub-optimal and therefore non-implementable and offered useless technological quick fixes that fell between all stools and instead of adding anything positive to India's cyber security strength, would have only increased the vulnerabilities many a time over.

Data Governance Algorithm

Even as in the immediate term India cannot match (such competencies are built over decades and sadly India has been somnambulant on the cyber security front since independence), the length, breadth and depth, pretty literally, of the operations of a "Stellar Wind", and while it might not be a model to be replicated in all ways as it might just be too sinister with too weak a mechanism of checks and balances, we can and should do a few things. Actually three things, specifically.

First, tell the technology companies operating in India that they would have to move their servers to India. Period. This way, the servers would fall within India's jurisdiction and with the help of enabling laws and in exercise of sovereign power, Indian government can then enforce data sharing programmes based on pre-set system of rules. We need to tell the technology companies that Cyberterrorism has become an overriding threat to India and if they don't comply the very integrity of highest growth and mammoth market that India is, which funds their expansion, stands in jeopardy. The tech biggies might do a bit of fretting and fuming but they'd comply to protect their market. In the bargain they'd pressurize the Narendra Modi government to socialize the cost of the shift. They'd forward the argument that servers work best when not held hostage to physical location. None of these arguments are valid as both the cost and the performance impact would be

negligible to miniscule. But considering the jobs that it might create in India, we might want to give them a few investment incentives.

We might not be running a “Stellar Wind” but we surely are running mammoth programs such as “Digital India”, “Make In India” and “Smart Cities” and these programs would technologically and architecturally work like magic in concert with the idea of moving servers to India. Infact one cannot imagine Smart Cities into the next century without robust data governance systems that offer a resilient city to live in that’s quarantined from terrorist attacks.

Most of all, if the citizenry’s argument against holding the decrypted data for 90 days as stipulated in the draft is that it is an attack on privacy (and it is a valid argument), then that argument would apply with exponentially, nay, astronomically greater force on keeping their data in servers outside India forever (as is significantly the case right now). Bringing the servers into India should therefore be welcome by Indian citizens because right now their data is vulnerable in the hands of American government, let alone the Indian government. In short it would be a political cushion for the Narendra Modi government. The Narendra Modi government can tell the Indian people that it shall be ensuring a far greater protection of the data of Indians by bringing the servers home.

I know bringing the servers home is easier said than done. But nobody said running a nation the size of India and protecting it from ever increasing and new technologically complex threats was going to be easy. Once the servers are all here, a lot or all of the government’s trouble with encrypted data would be tackled. Remember that USA, even with Stellar Wind is unable to get all the data it wants without having to request technology companies for data cooperation and the technology corporations still display their inability to cooperate, in spite of court orders, citing technological infeasibilities.

Secondly, the government would need to set up ‘checks and balances’. These would be policies on when the event of targeting specific users would arise as against the normal, steady state anonymous scooping of data that would be analysed for anti-national, terror oriented chatter without invoking future privacy clauses. This should not be a huge challenge at all, as right now cellular phones are snooped on legally in India, where the snooping does get individualistic rather than anonymized. A similar legal process that is adapted to the idiosyncrasies of the cyberworld would need to be put in place. However, those pockets of the web that are popularly known as the “Deep Web” or the “Darknet”, the underworld of the world wide web where illegal wares are transacted, should be exempt from the application of such checks and balances.

Thirdly, and last but not least, developing cyber intelligence systems should become the core focus. The entire policy would look good on paper alone if we haven’t an institutionalized cyber intelligence effort in place. In fact, this would speak beautifully to the “Skill India” program of the Narendra Modi government. One can leverage on the latent strength of highly skilled Indian programmers, arguably the best in the world, and integrate them in the effort and create the most powerful army of computer programmers. This itself might have positive unintended spin offs that could unleash cyber innovation, thus adding to the economy.

A word of caution would be that such programmers must be vetted and the government must not commission an organization that might have even an iota of conflict of interest. For example, if an organization, no matter howsoever “Indian” it might be, has been engaged by external security agencies such as, say, FBI, then such organizations ought not to be involved in developing an Indian version of the Stellar Wind in anyway whatsoever. Such operations simply cannot be outsourced and must be inhouse, built ground up by the agencies of the government.

This should not be very difficult and considering that the Narendra Modi government is progressing in the direction of developing cyber capabilities indigenously, as evident in mainstreaming an indigenous, highly secure computer operating system named BOSS – Bharat Operating System Solutions. BOSS would replace Microsoft Windows, most likely because Windows is considered an obvious vulnerability and would be our first and defensive step in cyberwarfare. The next level of the discourse would be developing a cyber intelligence system that would be the offensive system, where we shall be in hot pursuit of cyberterrorists. And we’d be home!

One hopes, trusts and prays that these words would ring closer to home and appropriate action would be taken to set the discourse onto the correct path.

Bibliography

Bamford, James (15 March 2012), *The NSA is building the Country’s Biggest Spy Center (Watch What You Say)*, Wired Magazine. http://www.wired.com/2012/03/ff_nsadatacenter/ (28 September 2015)

Vink, Jorick S. (5 December 2011), *The Theory of Stellar Winds*, arxiv.org, Cornell University Library. <http://arxiv.org/pdf/1112.0952v1.pdf> (28 September 2015)

DeiTY: Department of Electronics and Information Technology, Ministry of Communications and Information Technology, Government of India (21 September 2015), *Draft National Encryption Policy*. Note: the draft has now been withdrawn. <https://info.publicintelligence.net/IN-DraftEncryptionPolicy.pdf>. (28 September 2015)

Express News Service (23 September 2015), *Criticism forces government to rollback its draft encryption policy*. Indian Express. <http://indianexpress.com/article/india/india-others/government-withdraws-draft-national-encryption-policy-after-furore/> (28 September 2015)

Mankotia, Anandita Singh (23 September 2015), *Encryption policy poorly worded by officer: Telecom Minister Ravi Shankar Prasad*. Economic Times. <http://economictimes.indiatimes.com/>

tech/internet/encryption-policy-poorly-worded-by-officer-telecom-minister-ravi-shankar-prasad/articleshow/49068406.cms. (28 September 2015)

PTI: Press Trust of India (22 September 2015), *Data encryption policy slammed by opposition parties*, The Economic Times. <http://economictimes.indiatimes.com/news/politics-and-nation/draft-encryption-policy-slammed-by-opposition-parties/articleshow/49061451.cms>. (28 September 2015)

Wood, Collin (29 April 2014), *Data Governance: The Public Sector's Next Big Frontier*, GOVTECH.COM. <http://www.govtech.com/data/Data-Governance.html>. (28 September 2015)

Weimann, Gabriel (December 2004), *Cyberterrorism: How real is the threat?*, United States Institute of Peace. <http://www.usip.org/sites/default/files/sr119.pdf>. (28 September 2015)

Pizzi, Michael (7 January 2014), *Cyberwarfare greater threat to US than terrorism, say security experts*, Alzazeera, America. <http://america.aljazeera.com/articles/2014/1/7/defense-leaders-saycyberwarfaregreatestthreattous.html>. (28 September 2015)

Gellman, Barton (12 May 2011), *Is the FBI Up to the Job 10 Years After 9/11?* Time. <http://content.time.com/time/magazine/article/0,9171,2068082-4,00.html>. (28 September 2015)

Lohrmann, Dan (18 May 2015), *How Dangerous is the ISIS Cyber Caliphate Threat?*, GOVTECH.COM. <http://www.govtech.com/blogs/lohmann-on-cybersecurity/Cyber-Terrorism-How-Dangerous-is-the-ISIS-Cyber-Caliphate-Threat.html>. (28 September 2015)

Graham-Harrison, Emma (12 April 2015), *Could ISIS 'cyber caliphate' unleash a deadly attack on key targets*, The Guardian. <http://www.theguardian.com/world/2015/apr/12/isis-cyber-caliphate-hacking-technology-arms-race>. (28 September 2015)

Thomas, Pierre; Levine, Mike (26 July 2015), *Why Attorney General Says ISIS Is More of a Threat Than al Qaeda*, abcnews.go.com. <http://abcnews.go.com/Politics/attorney-general-isis-threat-al-qaeda/story?id=32691727>. (28 September 2015)

Bruer, Wesley (12 May 2015), *NSA director says ISIS ideology 'increasingly resonating' with Americans*, CNN. <http://edition.cnn.com/2015/05/11/politics/nsa-cyber-terror-isis-recruitment/>. (28 September 2015)

Bennet, Cory; Viebeck, Elise (17 May 2015), *ISIS prepares for cyber-wars*, TheHill. <http://thehill.com/policy/cybersecurity/242280-isis-preps-for-cyber-war>. (28 September 2015)

Madden, Mary (12 November 2014), *Public Perceptions of Privacy and Security in the Post-Snowden Era*, Pew Research Center. <http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/>. (28 September 2015)

Karam, Joyce (14 December 2014), *Shami Witness Arrest Rattles ISIS Cages on Twitter*, Al Arabiya News. <http://english.alarabiya.net/en/perspective/features/2014/12/14/Shami-Witness-arrest-rattles-ISIS-cages-on-Twitter.html>, <https://twitter.com/ShamiWitness>. (28 September 2015)

Apuzzo, Matt; Sanger, David E.; Schmidt, Michael S. (7 September 2015), *Apple and Other Tech Companies Tangle With U.S. Over Data Access*. http://www.nytimes.com/2015/09/08/us/politics/apple-and-other-tech-companies-tangle-with-us-over-access-to-data.html?_r=0. (28 September 2015)

Unnithan, Sandeep et al (9 December 2010), *The Secret World of Phone Tapping*, India Today. <http://indiatoday.intoday.in/story/the-secret-world-of-phone-tapping/1/122693.html>. (28 September 2015)

Rahooof, KK Abdul (15 June 2015), *Hyderabad Criminals in Deep Web*, Deccan Chronicle. <http://www.deccanchronicle.com/150615/nation-crime/article/hyderabad-criminals-deep-web>. (28 September 2015)

Maharishi, Phalgunn (15 September 2015), *Indian govt's new Bharat Operating System likely to replace Microsoft Windows*, ABPLive. <http://www.abplive.in/gadget/2015/09/15/article715008.ece/Indian-govts-new-Bharat-Operating-System-likely-to-replace-Microsoft-Windows>. (28 September 2015)