The Theory of Regulated Anonymity

Naavi

The theory of regulated anonymity as propounded by Naavi advocates a conflict resolution solution for preserving the democratic principles of Privacy Protection in Cyber Space along with the need of the law enforcement to be able to prevent misuse of "Privacy" as a cover for Cyber Crimes.

Internet developed in the 70's because of its ability to provide an opportunity for anonymous expression by individuals. Even today Privacy activists are fighting for anonymity as a matter of right. "Right to be Forgotten" is the new prescription of privacy laws under development in EU.

There is admittedly, a strong case for "Anonymity" and also "Pseudonomity" as means of protecting the privacy of an individual on the Internet. However looking from the perspective of increasing Cyber Crimes and their escalation to Cyber Terrorism and Cyber Wars, there is an equally strong case for the demand of the law enforcement for absolute surveillance and need to identify individuals conducting any transaction on the Internet. The new laws in most countries including India and US try to provide for such " Authorized Invasion of Privacy". This brings forth the direct conflict between Privacy and Crime Prevention while formulating regulations.

If we agree that even "Democracy" needs to defend Cyber attacks on its individuals and therefore do everything within its powers to identify criminals and punish them if they are hiding behind the privacy rights, then it is necessary to find a solution to this conflict of interest.

The biggest problem in Privacy advocates accepting to any form of surveillance is the proven fact that a power meant to secure the society is always misused by the Government to secure its own power to rule. Thus, surveillance will be used to gather information on the activities of the political opponents and to intimidate the opponents. Thus a dictatorship under the garb of democracy can always use the powers assumed for national security of the security of the political party.

It is in this context of both “Anonymity” and “Regulation” having their own justification that I suggest a system of “Regulated Anonymity”. This could be a solution to resolving the conflict between Privacy advocates and the regulators.

The system of “Regulated Anonymity” envisages that a “Non-Governmental” body of the Netizens will regulate the anonymity. The system would be similar to the presently available “Anonimizer” services. However, at present the anonimizers are either run with a profit motive by a private company or known groups of law evaders. While an anonimizer run by a private company will only replace the Government with a private entity who can be corrupted for an organized breach of information, an anonimizer run by law evaders will not cooperate with the regulators even when it is necessary in the interest of the society.

We therefore need to have an agency which is not a Government body with political interests, nor a private body with profit interest nor a criminal body with self protective interests. It is a challenge of the “Regulated Anonymity” system to find such an agency.

The control should be with a distributed set of persons committed to Privacy and Safe Internet. The interaction of the law enforcement agency should be with people who are another set of persons who can evaluate the requirements of the law enforcement and invoke a trusted cooperation from the technical team to reveal the identity of persons behind any offending transaction.

Essence of the Theory

Naavi’s Theory of Regulated Anonymity is built on the premise that “Absolute Anonymity of the Netizen is impractical as it would be completely opposed by all law enforcement authorities and is against the current laws in most countries.

Under the theory,   Anonymity should be regulated by providing every Netizen with a “Cyber Space Avatar ID” to substitute the “Physical Space Citizen ID”.

The Netizen may use his Netizen ID whenever he wants to be anonymous while he is free to do any transaction in Cyber Space also with the Citizen ID of the Physical Society. Whenever a justification arises for the Privacy veil to be lifted, a due process outside the control of the Government/Politicians/Corporate interests would be applied.

The assumptions under this theory are

a) Government of the day is not absolutely trusted by the Citizens and

b) Privacy law in most countries advocate a “Due Process” for lifting the privacy veil in the interest of national security etc. However the “Due Process” has a tendency to get corrupted in favour of an aggressive Government or influential corporate authority.

c) There is a need for an agency to act as an “Ombudsman” (Privacy Protection Group or PPG) between the Law enforcement authorities and the Citizen to decide when privacy veil can be lifted in the interest of national security and in accordance with the due process of law.

d) PPG has to be constituted outside the control of the major stake holders in privacy breach namely the Government, Politicians, and the Corporate powers.

e) Anonymity can be better preserved by distributing data across multiple persons and locations so that no single country or single person has all the data that are necessary for identifying a Netizen of the Cyber Society to a corresponding Citizen in the Physical world.

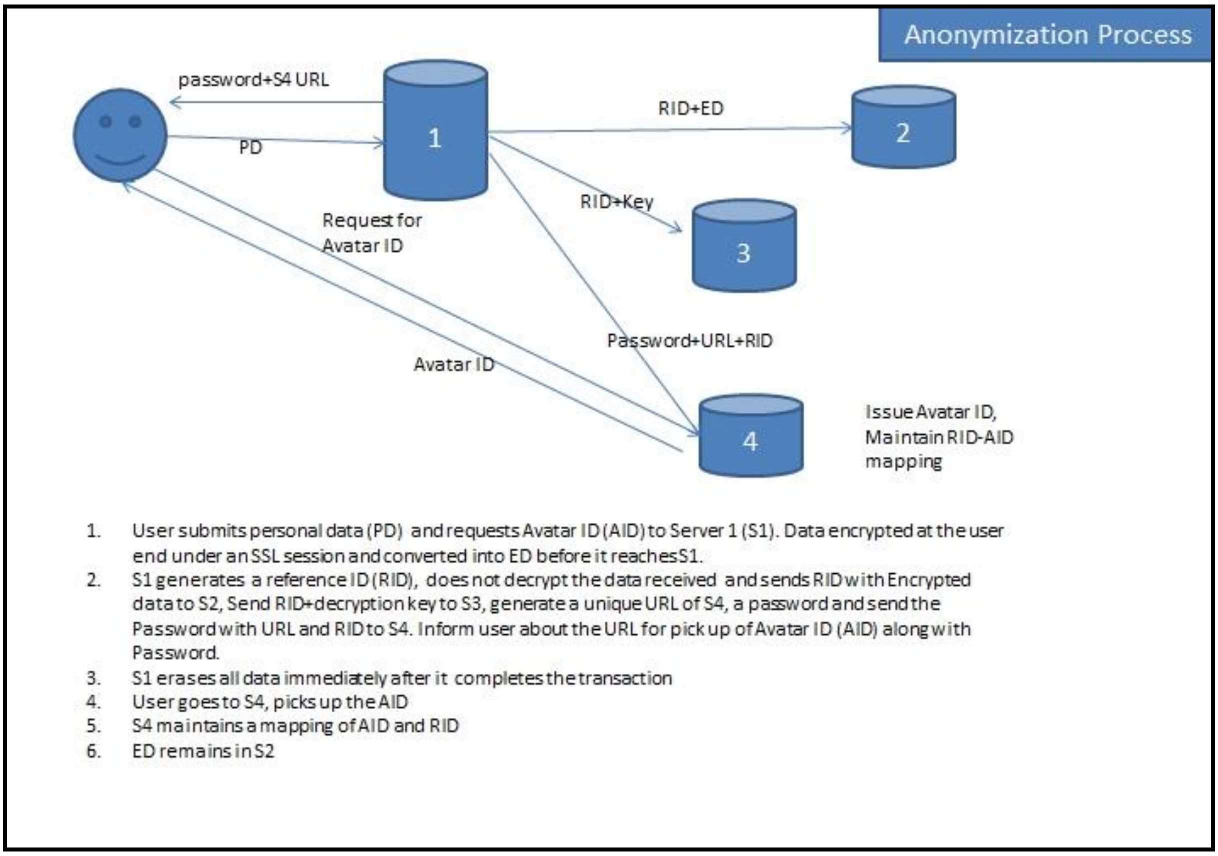
f) Necessary and Sufficient Penalties can be imposed on the Netizens applicable to Cyber Society independent of the penalties that can be imposed on the Citizen mapped to an offending the Netizen ID.

Suggested Process

In pursuance of the above principles, the system of Regulated Anonymity recommended by Naavi is depicted in the following diagrams.

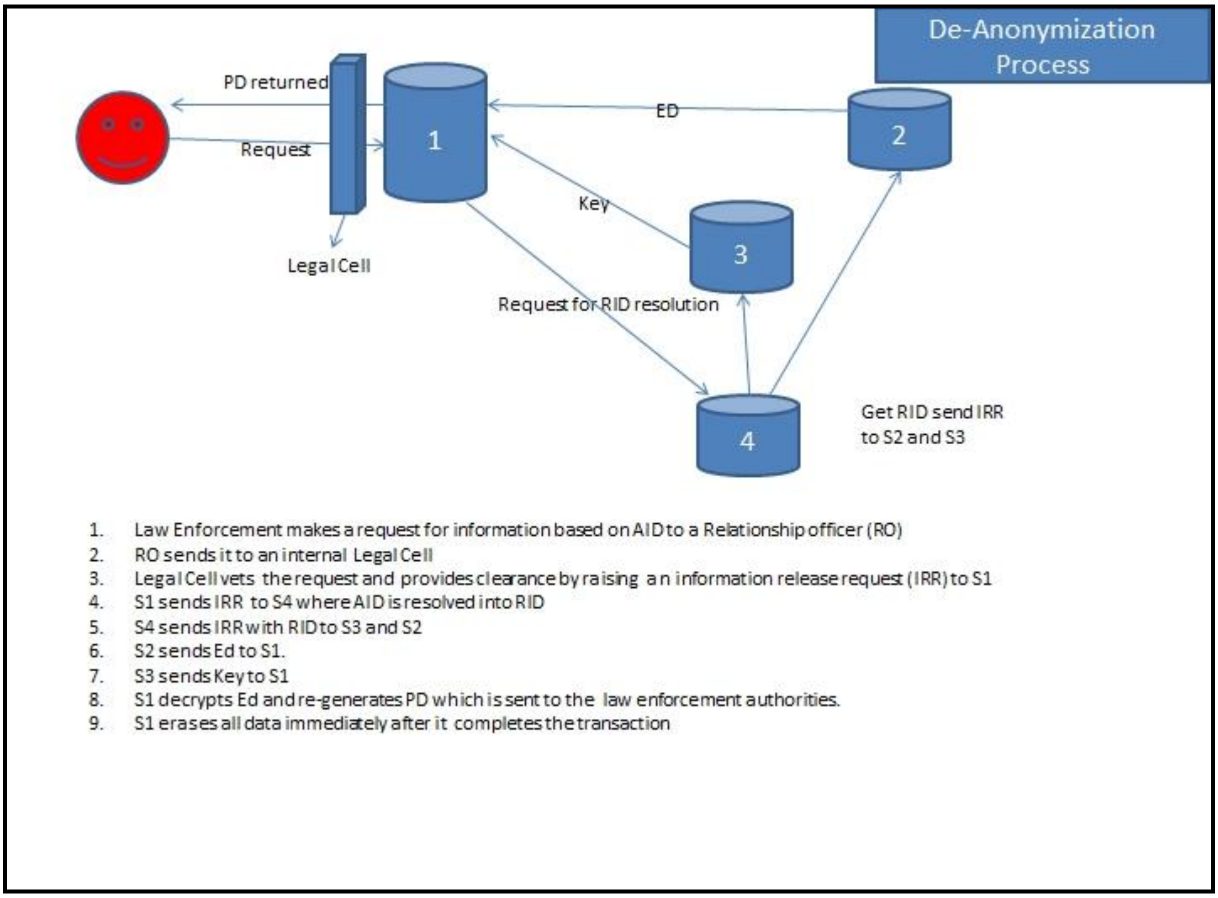
The first diagram shows the suggested architecture for converting the Citizen ID to a Netizen ID and the second diagram shows how the request for the lifting of the privacy veil will function.

Diagram 1



1. User submits personal data (PD) and requests Avatar ID (AID) to Server 1 (S1). Data encrypted at the user end under an SSL session and converted into ED before it reaches S1.
2. S1 generates a reference ID (RID), does not decrypt the data received and sends RID with Encrypted data to S2, Send RID+decryption key to S3, generate a unique URL of S4, a password and send the Password with URL and RID to S4. Inform user about the URL for pick up of Avatar ID (AID) along with Password.
3. S1 erases all data immediately after it completes the transaction
4. User goes to S4, picks up the AID
5. S4 maintains a mapping of AID and RID
6. ED remains in S2

Diagram 2



1. Law Enforcement makes a request for information based on AID to a Relationship officer (RO)
2. RO sends it to an internal Legal Cell
3. Legal Cell vets the request and provides clearance by raising an information release request (IRR) to S1
4. S1 sends IRR to S4 where AID is resolved into RID
5. S4 sends IRR with RID to S3 and S2
6. S2 sends Ed to S1.
7. S3 sends Key to S1
8. S1 decrypts Ed and re-generates PD which is sent to the law enforcement authorities.
9. S1 erases all data immediately after it completes the transaction

In the above process, only for a brief period, private data will be available in unencrypted form at any stage of anonymization. It will be encrypted before the end of the initial session in "Cache" form and moved into S2. The decryption key is not sent to S2 but is sent to S3. Once the session is closed, the unencrypted data gets deleted from S1. S4 gets only the RID and generates the Avatar ID.

The decryption occurs only at the time of disclosure after the approval of the PPG when S1 collates the RID from S4, Encrypted Data from S2 and decryption key from S3. This is sent to the law enforcement agency after which it again gets deleted from cache memory itself.

The servers would be in different countries other than the country of residence of the user.

This system ensures that data gets distributed over three/four different countries and servers and hence it would be difficult to forcefully access the data by any Governmental authority.

The process of revealing the personal data in case of a genuine need would be handled with a strong mechanism for filtering fake requests and unlawful requests. The body which filters the requests from law enforcement agencies will consist of experts in privacy law in different countries. It should be as strong as the ICANN and should be removed from the administrative control of any single Government. A body of multiple Governments such as the "Cyber-UNO" may be conceived to deal with any conflict between the physical society and the digital society arising out of the anonymity issues.

This process of Regulated Anonymity is expected to satisfy the Privacy requirements as well as the law enforcement needs.

It remains to be seen however who will venture into setting up the above system. It would be ideal that an organization like ICANN should take the lead in establishing such a system.

Naavi
naavi@vsnl.com
www.naavi.org
+919343554943