International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

Open Standards for Unified and Secure Data Privacy Policies in context of Trusted Social Networking

Varun M Deshpande[1], Dr. Mydhili K. Nair[2]

[1]PhD Student, Department of Computer Science & Engineering, Jain University, Bangalore, India
[2]Professor, Department of Information Science & Engineering, M S Ramaiah Institute of Technology, Bangalore, India

ABSTRACT

Social Networking sites(SNS) like Facebook and Google provide Free services to their users! They leverage on external revenue generating mechanisms. They even resort to 'leasing' out user generated data to third party entities such as data mining, data analytics companies etc. "So What?" - there is a chance that the data analysts or advertisers misuse user data (especially personally identifiable information) adversely. Each company creates their own privacy & data sharing policy which is subject to interpretation by their legacl teams. There is need to find workable solutions in order to ensure that there is no scope for misuse or privacy breach by companies. Privacy policies and legislations play a vital role in protection of data security and privacy of user's digital identity from being compromised. A holistic and technically sound policy is very important to set the expectations and regulations for service providers & law enforcement agencies in order to uphold the rights of users around the world. We believe that a unified secure data privacy policy for data sharing that are geo agnostic is a necessity for social networking. We propose Open Standards for such technically correct policies that include Certifying Agencies that audit the service providers in real time. These policies needs to be revised on periodic basis by including all relevant stake holders; and needs to be enforced on social networking service providers in order to move towards Trusted Social Networking.

Keywords: Privacy, Policies, Trust, Social Networking, Data Security, Open Standards, Unified Policy

I. INTRODUCTION

With advent of social networking era, communication and information exchange have become a defining element in today's information technology driven world. Each person is empowered as he can communicate with anyone in any corner of the world over the internet via the SNS such as Facebook and Google. As per recent published reports, both Google and Facebook have about 2 Billion monthly active users and well over a Billion daily users. There are similar number of daily users of online messaging service provider Whatsapp. With so many users communicating online, the amount of information exchanged is truly of mammoth proportions.

Above data shows how people around the world have embraced the era of social connectedness with open arms. It has become daily routine to check accounts on Facebook, Whatsapp or Gmail on a regular basis. Social networking has truly made tremendous difference for all our lives.

A. Why Should we worry about Privacy?

All this communication means that unprecedented amount of data is being generated by passing of each second. A good part of this data includes personal information such as one's likes and dislikes, location/check-ins, browsing history, email exchanges, photos, chats or messages, purchasing record, financial information, health related data etc. Some or all of these may be regarded as sensitive information (SI) or even

Personally Identifiable Information (PII). Essentially, it means that combining one or more data points in the available data set, such as gender, location, preferences etc., we may be able to personally identify the individual or organizations and use that information in any unfair way. Hence it is important to understand in detail what is the business model of the service providers and how they are treating the data collected from the end users of their services.

Online SNS that provide a convenient mode of interaction, which may pose some important privacy and data security concerns. Zhi Chang et. al. [1] discuss about the design conflicts in social networks related to usability and sociability which impede them from providing absolute control over user's privacy and data security. Azizul Yaakup et. al.[15] distinctly points out certain concerns related to Facebook advertising such as credibility of advertisers and privacy of users. Hence, user's privacy concerns are of utmost importance to study and understand.

B. Digital Identity and Data Security & Privacy

User's online activity along with their accounts created on various service provider websites form their digital identity. This influences how user is perceived by others in the community thus impacts how they interact and their build reputation [2]. Also, content displayed in websites are a function of user's digital foot print. Hence this has capacity to shape influence his or her decisions. There are even chances of one's digital identity being stolen by use of PII. Identity theft resulting from data/privacy breach is a serious cause of concern. Hence addressing the privacy and data security concerns in digital identity management has become more relevant than ever before.

C. Scope of Current Work

In current work, we concentrate our focus specifically SNS and e-commerce sites that provide software as a service usually at free of cost to end user such as Facebook, Amazon and Google. These services are hosted on cloud servers that are maintained by the respective companies. They address all the security challenges of cloud computing along with privacy and data security concerns. In these kinds of cloud based services, it is the service provider who defines the privacy policy and related norms. Privacy laws also need to adhere with some of the legal requirements of the law of land.

It is often the case that privacy policy and terms & conditions are lengthy legal writings that users hardly pay attention to it. Users of the service have no choice but to comply with the terms and conditions. They do so as they are rewarded by convenience of connecting with people around the world or to shop at click of a button. On the other side of this arrangement, service providers benefit by providing advertisements based on user generated content. They make money when user clicks on such links and visits, or purchases product/service from the advertiser. In this way, social networking sites influence user's digital behavior.

Control of user's data is completely shifted to cloud service provider. They act as the proxy owners of data. Hence, there is always a lack of trust with respect to data handling in cloud server. General view is that user's data is vulnerable for intentional or unintentional disclosure/theft. Cloud service providers may face a data breach from external hackers or they may intentionally or unintentionally share some amount of PIIs with 3rd party clients such as advertisers or data providers. Hence there is an urgent need for finding holistic and trustable solutions for issues around privacy and data security when it comes to digital identity management in cloud based services.

Current research work is one of many such ongoing important works dealing specifically with privacy and data security concerns in social networking space from a privacy policy perspective highlighted as below.

- **Review the literature on current topic (**Section II**)**
- **Understand privacy laws in different geographies and their short comings** (Section III)
- **Analyze the cause and effects of user's privacy concerns** (Section IV)
- **Propose Open Standards for unified and secure data privacy policies in context of Trusted Social Networking** (Section V)

II. REVIEW OF LITERATURE

A. Privacy Definitions, Litigations and Considerations

It is true that lot of research has been in the domain of privacy [10] [11]. However, there needs to be academic

discussions on the privacy policies of the service providers as well as state policies around the privacy and data security laws and regulations. Without this, the discussion would not be complete.

Privacy has been an issue debated by Deyan Chen, Hong Zhao. In their work [3], they provide analysis of current solutions in the field of data security and privacy issues in cloud computing. They discuss about the concerns which exist during handling of data which is sensitive during the data life cycle. It consists of following phases: ***generation, transfer, use, share, storage, archival and destruction***. They highlight that although regulatory bodies have developed rules for data sanitization, they have not provided the implementation details for the same. They direct that future work should be focused on separation is sensitive data from other data, data access control mechanisms and identity management.

Rein Turn [4] defined privacy in context of automated record-keeping systems dealing with personal information as, "*rights of individuals regarding the collection, storage, processing, circulation and use of personal information about themselves*".
He was of opinion that privacy protection can be granted only when it is backed by legislative laws and/or by the record keeping organizations. We concur with his observations and mark that official regulations can only bring about strict enforcement of any policy. He also discussed what can be regarded as privacy violation defined as per legal community. He surveyed status of privacy protection issues at that time as well as listed future issues for privacy protection. There were a few legislations passed in USA during 1970's including Privacy Act of 1974, Electronic Funds Transfer Act of 1978 etc. They placed certain technical requirements for ensuring data quality, implementation of access control as well as security measures and provide auditing compliance. They felt that there was a growing pressure from public users of computer systems for eventual strengthening of privacy protection laws as new technological capabilities would impact personal information collection.

Rein Turn [5] a decade after his previous work [4], marks that information privacy deals with protecting individual against potential violations of their rights due to collection, storage and use of personal information by private and government institutions. He is of opinion that privacy protection legislative laws enacted during 1970's are inadequate and have limited scope. The emergence of newer technologies during 1990's could potentially result in privacy violations in newer ways. This warrants research and understand the requirements of new privacy laws. Shortcomings of existing laws included no effective enforcement mechanism, considerable scope for interpretation, broad exemptions provided to intelligence agencies and that burden of execution of privacy protection rights were placed on individual. New technologies emerging in 1990's such as electronic mails were designed to automatically store personal data as bi-product of service provided, automated decision making systems based on the stored data of individuals.

Author envisioned that future legislations should understand the capabilities of upcoming technologies and accommodate them. Technical measures to protect against unauthorized usage to enforce accountability and security effectiveness. Ethical standards, education and training are need of hour. Also, there is need for "***Watchdog***" groups of computer science professionals and media to uphold rights of individuals against misuse of laws.

We have come a long way since this paper was published in 1990. Yet, today researchers still are striving hard to address some of the digitally evolved privacy and security related research questions.

B. Digital Identity and Sensitive Information

Dongxi Liu et. al. [6] take up the problem of privacy preservation of data outsourced by organizations for data analytics purpose. It is very convenient to share data with some other organization. However, it may lead to privacy breaches and sensitive information leakage. Authors propose a mechanism where data owner can use homomorphic encryption for encrypting the data. Later use k-means clustering over this. To simplify the process of comparing encrypted distances, they propose to use trapdoor information provided by data owners. As a future work, authors say that current distributed k-means clustering could be combined with outsourced k-means clustering to making it more secure.

Eliza Bertino[20] underlines that privacy preserving digital identity management is key for secure use of internet and online applications. Problem of Identity

theft has grown beyond bounds in cyberspace. Per author, digital identity can be defined as "*the digital representation of information known about an individual or party. Such information, referred to as identity attributes, encompasses not only attributive information, such as social security number, date of birth, and country of origin, but also biometrics, such as iris or fingerprint features, and information about user activities, including Web searches and e-shopping transactions*." Identity can be broadly classified as any personally identifiable information. Further author discussed challenges in this field of study and some of the considerations that need to be considered.

III. PRIVACY LAWS IN DIFFERENT COUNTRIES

One of the challenging element of privacy and data protection standards' enforcement is that, the laws have evolved differently in different countries in the world. Services make use of cloud data centers which speed across multiple geos to provide users a rich and responsive experience. This essentially means that users data may be transferred between multiple geos which are governed by different law enforcement policies. Hence to do business, the service providers need to comply with the different standards in different countries. Otherwise, it may attract large amounts of fines and/or losing of business.

There have been number of instances where companies have gone through these processes. This is damaging to the brand name and affects the trust of the consumers on the product. In *each of these cases, the kind of privacy breech were different which needs to be dealt with differently.*

A. Privacy Breaches in recent times

In this section, we look at some of the recent notable privacy breaches which ended up in litigation and fines. In 2014, Oi was fined over 3.5 Million Reais ($ 1.59 Million) by Brazil Government for violating its user's privacy. In this case, company was accused of collecting user's data without notifying them precisely what it was intending to use it for.

In the same year, Federal Communication Commission (FCC) intended to fine telecom service providers TerraCom and YourTel with $10 Million for storing PII's in public domain which would be accessed by general internet search compromising user's privacy. This may have been a technical mistake which cost the company lot of money later for compromising user's data security/privacy.

In 2013, Google had to agree to pay a hefty $7 million to 38 states of USA including District of Columbia after a 3-year investigation. It had collected private data with its street view vehicles. While trying experiments for new products, we may cross the sensitive line of dealing with private data. Companies must be very careful about it.

In 2015, FCC fined AT&T with $25 million as an investigation found out that few of its employees sold personal information of significant number of customers. In such cases, even though the fault is from an individual or group of individuals, the blame and the bad name goes to the company overall for not setting up protocols for effective access control and data protection.

In September 2016, Yahoo declared that around 500 million users were leaked which had sensitive data stolen for 2 years. The attacker could gain access to PII and digital identities of the affected accounts.

In total, there have been at least 5,754 data breaches between 2005 and 2015 that have compromised 856,548,312 records. [20]

B. Privacy Laws in India

One can track the evolution of privacy laws in India with the information provided in official website of Department of Electronics and Information technology (DeitY) [14]. Based on the resolution taken at General assembly of United Nations in the year 1997, named "United Nations Model Law on Electronic Commerce 1996", India passed IT Act in year 2000. This was the first attempt at setting legal regulations, definitions and boundaries with respect to privacy and data security including online activity and cybercrime. Several amendments have been made to this act since then. Amendment Act of 2008 reformed some of requirements for collection, storage and usage of sensitive information and streamlined legal procedures if service providers fail to comply. However, user privacy related legislations remain to be largely

ambiguous and subject to interpretations especially related to surveillance.

C. Comparison between EU and US Privacy Laws

In a study comparing between US and EU data protection legislations, Prof Dr Franziska Boehm [7] has submitted a report to the European Parliament, as requested by the committee on Civil Liberty, Justice and Home Affairs (LIBE). In his report, he clearly underscores the philosophical differences between the policies. Author believes generally; EU has a more comprehensive data protection guarantees. On the contrary, US laws empowers US agencies to process personal data.

He also goes on to say that constitutional protection against data protection is limited under 4th amendment of Privacy Act for US citizens. It is subject to limited interpretation and generally favors the law enforcement agencies in view of national security interests. Majority of data protection standards which are present in EU are missing in US law such as sharing of PII information between agencies etc. is done only on need to know basis and requires justification in EU. While the same is sort of a rule to exchange information for inter department collaboration in the US. Even the newly added legislations in US such as Draft Judicial Redress Act of 2015 or the FREEDOM Act don't essentially change these philosophies but only partially improve the current situation bringing in stricter access requirements.

D. Analysis of Privacy Laws in Different Geos

Privacy laws in different countries vary based on the culmination of various factors including social, cultural, economic, geographic, and current affairs. Therefore, we see difference in the fundamental philosophies by which privacy and data protection laws are being framed or amended.

However, by the passing day, the world we live in is becoming a global village and the turning flat breaking down the physical barriers through virtual relationships and collaborations. For this reason, countries need to come together and frame a comprehensive data sharing, privacy and protection laws that collectively govern the entire jurisdictions. "**Umbrella Agreement**" [8] which was initiated in 2015 is one step towards such an arrangement between USA and European Union (EU). There has been demonstrated interests from EU to understand data protection laws of India [9]. We may expect similar level of agreements such as "Umbrella Agreement" between EU and India in near future. It is recommended that United Nations Organizations or the country collaborations such as G20, SAARC, BRICS, take up active role and responsibilities in unifying some of these data protection and privacy laws and move towards meaningful collaborations in this regard.

IV. Analysis of Discussions

A. Real-world Perspective

No person would like to live his daily life in a glass house. Each of us, have a boundary where our public life ends and private life begins. In real world scenario, we respect each others privacy. It is fround upon if we fail to do so even if it is in the best interest of the other person. This is how the society functions where evesdropping into a personal conversation is considered to be invasion of privacy. Corelating this with the digital world, we have, in a way, outsourced our personal privacy to the service provider. Users are data generators for the service providers who analyse the data to provide customized tailor made content and advertisements. This is the current eco-system that we live in, digitally. Hence, it becomes very important to understand the ever evolving privacy policies of governament and service providers.

Even though most of the service providers provide their service free of cost to the users, it has to be noted that they are extenssively using data collected by users for commercial purposes and making a lot of money from it (Facebook's Q1 2017 revenue was $24.7 Billion). Greater the number of users, greater are the profits of the company. Therefore, as valuable customers or academic researchers or industry speacialists, we have a moral responsibility to collectively understand, review and propose solutions to build better eco-systems where user's privacy is preserved in a holistic manner without disturbing the existing business model of service providers [21].

B. Privacy Issues: Cause and Effect

In the above sections, we have seen different perspectives on data privacy and security issues. Below

Fish-bone diagram (Figure 1) summarises various causes for the concern for user's privacy.

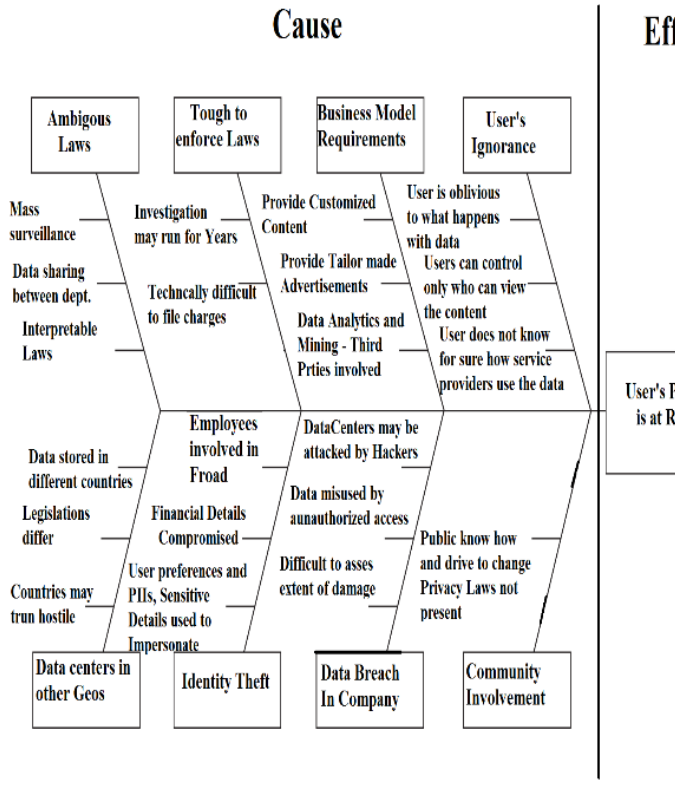

Figure 1: Privacy Issues: Cause and Effect

Some of the major contributors to the risk of user's privacy are as follows:

User's ignorance: Most of the times, user don't read through the privacy policies or terms & conditions and trust the service provider. This may be because, they know of many friends using the product, a friend recommended the product, or you just trust any company selling products to you and assume that they are "following the rules" in good faith. Awareness is key, and to provide mechanism to empower users to take educated decisions on their privacy settings such as Vidyalakshmi et. al. [12] discussion on providing privacy score to users and Varun M Deshpande et. al.[13] enabling users to decide what is best for themselves my go a long way in addressing this issue.

Business model requirements: Azizul Yaakup et. al.[15] discuss concerns with online advertisement. There is need to find workable solutions at root level to ensure that there is no scope for misuse by rogue 3rd party companies while keeping business model intact. Such a model was discussed by Varun M Deshpande et. al. in their work [22].

Tough to enforce laws: Unlike physical substances, the theft of soft data is not very apparent as the data is still present even after someone reads or makes copy of it. Hence it is technically challenging to ensure data integrity. Kiran et. al.[16] discuss ways of anonymization of private data using anonymization techniques. Companies and governments are advocating and enforcing strict access control mechanisms in order achieve this.

Most dangerous of attacks are the ones which we are not aware of. Mode of digital attacks are evolving at a rapid pace. Stuxnet worm [18] is one such example. Most effective wars can be fought by attacking the most mission critical aspects which provides a digital identity of an individual or a corporation or even a government. Hence it becomes even more important to look at this issue with help of industry specialists, academic scholars etc. and find good solutions.

Ambiguous Laws and Laws in different Geos: This issue has been in contention since initial days. Hence, each country is in constant review and amendments to the original laws based on recommendations or new requirements. One of the ways of addressing these issues at a high level is to define clear, unambiguous, technically correct legislations that ensure digital privacy. Current legislations are found to be very lacking in this regard, even at its best. Some of the attempts such as "***Right to be forgotten***" [17] are trying to help users to legally request for removing some of the undesired content related to them from search results. However, the cause of concern with this approach includes enormity of the number of such requests. Also, these altered search results are limited to servers in specific geos only and not globally. Hence, this defeats the intended purpose. Most countries don't even have well defined privacy and data protection laws. Also, these laws are different in different geos. So, there is certain ambiguity about data rights when the service providers process personal data in data centers of different countries. We believe that all countries through UN general assembly or groups and countries such as SAARC, BRICS, G20 etc. could come together and discuss about these concerns and have transparent regulations in interest of global citizens. There have been few good steps taken in this regard such as "Umbrella agreement" between EU and US. However, more such steps are welcome.

Identity Theft and Data breach in Company*:* It is a well-known fact now, that data security and privacy beaches are not just cause of concern for personal identity; but also organizations and even governments as a whole. We have seen several instances of such data breaches in recent times. Sony & Yahoo, being the most recent and notable ones. Hidden costs of such breaches will accumulate over years. Major concern is that it is very difficult to detect the same, as data is not a physical entity that disappears once stolen. Hence, in many cases, the victims are not even aware of espionage attacks until it has resulted in significant financial loss. Whenever we share our personal information such as health records, financial details or any PIIs online for various purposes, we hope that these are securely maintained. However, at back of our mind, there is always a concern of data breach in the service provider whom we are trusting.

V. OPEN STANDARDS BASED UNIFIED POLICY FRAMEWORK

A. Need for unified policy framework

Currently, the service providers are given autonomy to phrase their own privacy and data policy. There are certain high level guidelines that they need to adhere to the policies and law of land. We have seen that, in service providers use this as opportunity to define their own ways of declaring the policy. Effectively, user's privacy is leased out to the service provider. There are instances where service providers interpret that mere usage and accessing the service is a consent to use user's private and personal information as per their need [23].

We have discussed in above sections on how the governmental regulations and policies differ from one country to another. This is a cause of concern because the most of service providers are multinational in nature. Hence, the data travels the data centers located in one country to another. Google's legal battle in Brazil[24] is an example for this. Hence there is a need to start thinking of geo agnostic privacy policies which needs to be globally handled. Hence, there is a requirement for unification of certain globally acceptable and enforceable data sharing and privacy laws.

It is also noted that some of the privacy related laws are tough to enforce and audit. The privacy breach gets detected only after the fact and after enough damage met to the service provider and its user base. For this reason, a holistic, technically correct, auditable in real time policy framework is required.

Therefore, a unified structure for forming and implementing secure data privacy policy for data sharing is the need of the hour. All stake holders need to discuss and agree upon Open Standards for such technically sound policies. Implementation should be auditable in real time. These policies need to be revised on periodic basis by involving all relevant stake holders. It needs to be enforced on social networking service providers to move towards Trusted Social Networking.

Note*: Data sharing in social networking can be broadly classified into 2 modes. First one is through data aggregation and sharing totalitarian user base data with 3rd party for data analysis etc. Second mode is real time data sharing with 3rd party such as advertisers and advertising frameworks. This happens on the fly when user is interacting with the service provider. Our model deals with the 2nd mode or data sharing, i.e., real time data sharing on service provider's portal.*

B. Stake holders

Some of the major stake holders for developing Open Standards for Unified and Secure Data Privacy Policies for Social Networking involve below entities:

- Global body such as United Nations Organization (UNO) to govern the committee
- Representatives from governments of various Geos/countries
- Representatives from major service provides and market leaders
- Representatives from major Security Service Providers
- Representatives from leading Security researchers and academicians
- Representatives from major 3rd party advertisers & Vendors
- Representations from user community and subject matter experts

C. Role of Certifying Agencies

Varun M Deshpande et. al. [23], [22] have discussed about trust based data sharing policy framework in which a major component is proposal to include a component called as "Certifying Agency" (CA). Drawing from example of digital certificates and HTTPS encryption, a CA is a certified auditor who continuously audits the data sharing mechanism to and from service provider and 3rd party agent as shown in figure 2.

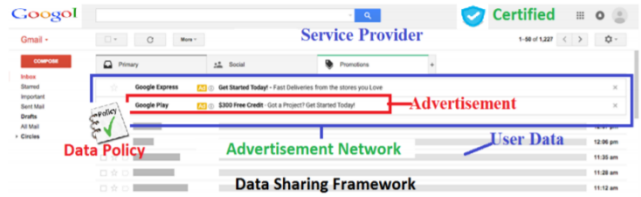

Figure 2: Secure Data Sharing Framework

- To implement this framework, a service provider needs to publish itself with a recognized CA. CA, provides code libraries and API keys to establish connection from the service provider and CA as shown in figure 3.

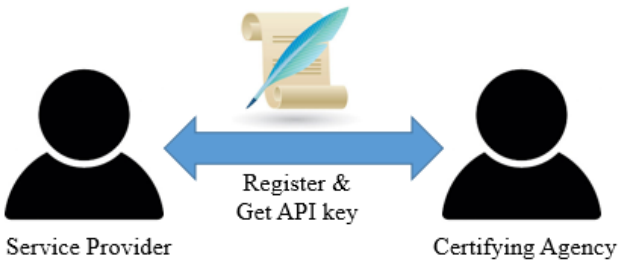

Figure 3: Service Provider Registers with CA

- Data sharing from service provider's website to and 3rd party needs to be done via the CA code libraries only using API key for authentication.

- CA then checks if the data is anonymized to a prescribed extent before sharing with 3rd party which is in the other end of data pipe as shown in figure 4.

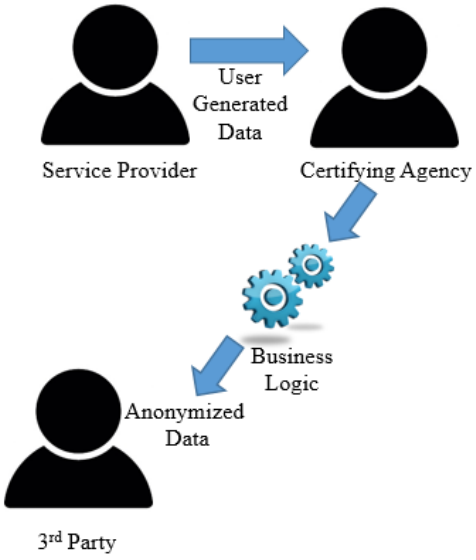

Figure 4: Secure Data Pipe

- CA handles enforcing secure data communication between service provider and 3rd party.

In traditional approach, a certifying agency would not interfere with the working of the system itself. However, in our approach, we have extended the responsibilities of CA. It should still be noted that CA would not directly work on the user generated data. It is only ensuring that a secure channel is provided for data sharing between the service provider and 3rd party. The business logic needs to be built in such a way that user generated data in anonymized and safe to be shared with the 3rd party. That part is not part of current scope and it would be dealt with in future work.

D. Recommendations

Data sharing and privacy policy is a sensitive subject. We need to hear from all the stakeholders and ensure that no body is targeted and everyone is given a chance to go about their business and excel at it. Here are few recommendations with respect to creating, implementing and maintenance of unified privacy policy for data sharing.

- All stake holders need to be consulted during formulation of data policy. This can be best done only under the umbrella of United Nations.
- A motion needs to be passed and all the sovereign countries need to state their support

for this cause and invest time, effort and money for this initiative (this re-usable model can be replicated in other segments as well such as health care/insurance etc.)

- All stake holders should be taken into confidence for a successful policy implementation
- All stake holders should agree upon certain data polies to be geo agnostic and a global standard
- Mission of data policy should always be to keep user's privacy requirements at the fore front of all the requirements
- Data policy should not adversely affect legitimate business models. They should try to make it possible for them to grow organically
- Data Policy needs to continuously evolve based on new technologies and business models
- Data policy needs to be reviewed in a regular period of at least 6 months
- Data policy should be holistic, technically correct and auditable in real time. i.e. Certifying Agencies should be able to detect the adherence or non-conformance in real time.
- Certifying Agencies should be highly available service that need to be auditable by external auditing agents and should live up to said high standards and expectations.
- Service providers need to strictly comply with data policy and work with CA to make use of data sharing model to run their business
- An Emergency Incident Response Task Force needs to be set up to review any anomalies that are reported on the field and take immediate remediation efforts to resolve the same

E.Proposed Open Standards for unified data policy

Based on above discussions, we propose initial version of Open Standards which needs to be reviewed by all the stake holders including the research community and taken forward for implementation.

1. All parties – Service provider, Certifying Agencies,3rd Party should satisfactorily demonstrate that they follow OWASP secure coding practices [26]
2. All parties – Service provider, CA and 3rd party should demonstrate the usage of HSTS protocol in all the web pages [27]
3. Pre-defined User Profiles need to setup and user should be clearly communicated about it. Example: Varun M Deshpande et. al. [23] described 3 different profiles – Freemium, Standard and Premium. Each of them have higher standard of default privacy control. There might be payment involved for the same.
4. Users should be able to choose any one of the profile as per their requirement and affordability.
5. Certifying Agencies should setup an unambiguous process for service providers to publish themselves and get API key for data sharing
6. CA should publish the code binaries in all majorly used computer languages or provide a secure SOAP/Restful web service to connect with them for secure data sharing
7. CA should have 99.999% availability for their services
8. CA should be geo agnostic and all the user data that is being shared outside of service provider should strictly pass through CA
9. Certifying Agencies should be audited on a periodic basis and get re certified
10. CA should allow any new or additional anonymization models to be applied in data sharing layer. This is to further strengthen data anonymization; or add data indicators that could help 3rd party to provide better and more relevant advertisements
11. Security tokens should be shared between service provider using SHA256 or better encryption algorithm. One of the security token should be able to detect the user profile chosen and one other security token used as a master switch for data sharing of user data to any 3rd party.
12. CA logo and security status ("Secure" or "Unsecure") should be prominently displayed in all the sponsored segments of the portal
13. Service provider portal should be scanned for web security vulnerabilities on real time for any outbound traffic leading to 3rd party without being intercepted by CA.
14. Any anomaly should be reported to Emergency Incident Response Task Force to review and act

VI. CONCLUSION AND FUTURE SCOPE

SNS have been successful in attracting large amount of user base to use their products regularly. Both Facebook and Google have over 1 Billion daily active users. The revenue generating mechanisms employed by them using data sharing and leasing model is a cause of privacy concern.

SNS and e-commerce services have been publishing their own privacy policy. This can lead to privacy breaches which take time to detect and are followed up by litigations and throw the SNS in bad light.

Some of the privacy laws which are in place in different geos are not holistic and are subject to interpretation. This causes avenues for disagreement between service providers and governmental agencies. This leads to litigations and friction for doing business with ease.

Over and above, the user needs to be able to trust the service provider with their personal information. Hence, unified privacy preserving data sharing policies are very much required to represent the needs of the end user who has most to lose in this situation.

In this data driven era of social networking, fueled by ever flowing gush of user generated data; security researchers have a moral duty to perform. As security researchers, we need to develop secure systems by which users can communicate with each other, stay connected and make new friends & relationships.

Open Standards for Unified and Secure Data Privacy Policies in context of Trusted Social Networking are needed to bring all the stake holders in a single round table meet and have them discuss the emerging privacy concerns and formulate legislations which would be implemented globally.

Technically correct laws which are auditable in real time and secure help in creating a sustainable environment for maintaining such a novel system. We are proposing towards unification of privacy laws and mandate them as a global standard and legislation to put user's privacy as number one priority.

Varun M Deshpande et. al. [22], [23] have discussed and shown how a unified policy framework could mean better business opportunities for service providers as well. Hence, we can conclude that such a system has high potential of being a Win-Win situation for all the stake holder.

Certifying Agency for data sharing policy implementation is a novel idea and creates a new segment of business which is currently not existing and the security companies can look up to providing the best solutions and attract the service providers towards them.

We have discussed extensively about various aspects that are cause of concern for privacy and data security to user's digital identity. We established that there is a need for comprehensive privacy & identity centric approach for solving these challenges. We then provided an approach to solve these problems. These models can be reused in health care and e-commerce.

We as research community have a unique opportunity to work towards ensuring digital privacy and identity. There is a technology space which is virtually unoccupied. From 10 years from now, there won't be thieves on the streets or in the banks. They will be among us looking for our most valuable asset-"Our Data". Current work equips us to face the concerns of tomorrow in a proactive manner.

As a continuation of current work, researchers should analyze the proposals for open standards & unified privacy policy and provide their insights and conclusions. Further work needs to be done in addressing anonymization techniques and data hiding algorithms in the data sharing component which will truly make the framework anonymous. Our further research direction is directed towards the same. We should further drive this framework for discussions in larger forums. This ensures that it reaches all the stake holders and have them discuss on implementing such a system and move towards trusted social networking. One more research area which is not dealt with in current work is how to ensure secure data sharing of aggregate data. This can be considered as a separate research direction.

VII. REFERENCES

[1] Chi Zhang, Jinyuan Sun, Xiaoyan Zhu and Yuguang Fang, "Privacy and security for online social networks: challenges and opportunities"

Published in IEEE Network Volume 24, Issue 4 in 2010, Pg 13-18

[2] Steven Warburton and Stylianos Hatzipanagos, "Digital Identity and Social Media", Published in 2012 by IGI Global. Print Isbn-10: 1-4666-1915-5

[3] Deyan Chen, Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", International Conference on Computer Science and Electronics Engineering, 2012

[4] Rein Turn, "Privacy Protection in the f's", Published in IEEE Symposium of Security and Privacy in 1982

[5] Rein Turn, "Information Privacy Issues for the 1990's", Published in

[6] IEEE Symposium of Security and Privacy, 1990

[7] Dongxi Liu, Elisa Bertino and Xun Yi. "Privacy of Outsourced k-Means Clustering", Proc. 9th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2014), Kyoto, Japan, June 4-6, 2014

[8] Prof Dr. Franziska Boehm, "A comparison between US and EU data protection legislation for law enforcement purposes" DOCUMENT REQUESTED BY THE COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS (LIBE), European Parliament, September 2015. Link: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf (Last viewed on 21st Aug 2017)

[9] http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm (Last viewed on 21st Aug 2017)

[10] http://ec.europa.eu/justice/data-protection/document/studies/files/final_report_india_en.pdf (Last viewed on 21st Aug 2017)

[11] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks." In Proceedings of the 2005 ACM workshop on Privacy in the electronic society, pages 71–80, 2005.

[12] N. B. Ellison, J. Vitak, C. Steinfield, R. Gray, and C. Lampe, "Negotiating privacy concerns and social capital needs in a social media environment.", In Privacy online, pages 19–32. Springer, 2011

[13] VidyaLakshmi B. S., Raymond K. Wong, Chi-Hung Chi, "Privacy Scoring for Social network users as a service", published in "2015 IEEE Inernational Conference on Service Computing", 2015

[14] Varun M Deshpande, Dr. Mydhili K. Nair (2014), Anveshana – Search for the Right Service, In Proceedings published by IEEE of International Conference of Convergence of Technology, Pune, Maharastra (India), ISBN 978-1-4799-3759-2

[15] http://deity.gov.in/ Department of Electronics and Information technology (DeitY) (Last Accessed on 22nd Feb, 2016)

[16] Azizul Yaakop et al., "Like It or Not: Issue of Credibility in Facebook Advertising", 2013 , Published by Canadian Center of Science and Education

[17] Kiran P et al., "SW-SDF Based Personal Privacy with QIDB Anonymization Method", 2012, International Journal of Advanced Computer Science and Applications

[18] SIMON WECHSLER, "The Right to Remember: The European Convention on Human Rights and the Right to Be Forgotten" published in Columbia Journal of Law and Social Problems, 2015

[19] P. W. Singer, "Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons", accepted for inclusion in Case Western Reserve Journal of International Law by an authorized administrator of Case Western Reserve University School of Law Scholarly Commons. 2015

[20] Elisa Bertino, "Trusted Identities in Cyberspace", Published in IEEE Internet Computing , Volume 16 Issue 1, 2012

[21] Varun M Deshpande, Dr. Mydhili K. Nair, Ayush Bihani, "Optimization of Security as an Enabler for Cloud Services and Applications", to be published by Springer in edited volume titled "Cloud Computing for Optimization: Foundations, Applications, Challenges", to be published in "Studies in Big Data" **book series**, **Springer** (2017)

[22] Varun M Deshpande, Dr. Mydhili K. Nair (2017), "A Novel Framework for Privacy Preserving Ad-Free Social Networking", published in Proceedings by **IEEE** of 2017 2nd International Conference for Convergence in Technology (I2CT), Pune, Maharastra (India), ISBN 978-1-5090-4307-1/17

[23] Varun M Deshpande, Dr Mydhili K. Nair, "Trust based Novel Secure Data Sharing Policy Framework for Social Networking", published in International Journal of Engineering Research in Computer Science and Engineering (IJERCSE), Vol4, Issue 6, June 2017, Online ISSN- 2394-2320, with Impact Factor 4.890

[24] https://www.flipkart.com/pages/privacypolicy (Last accessed on 21st Aug 2017)

[25] Google Faces Legal Hurdles Under Brazilian Internet Law : https://ccgnludelhi.wordpress.com/2016/11/30/google-faces-legal-hurdles-under-brazilian-internet-law/ (Last accessed on 21st Aug 2017)

[26] OWASP Secure Coding Practices Quick Reference Guide Link: https://www.owasp.org/images/0/08/OWASP_SCP_Quick_Reference_Guide_v2.pdf (Last accessed on 21st Aug 2017)

[27] HTTP Strict Transport Security Cheat Sheet Link: https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet (Last accessed on 21st Aug 2017)