Privacy is Dead

Abstract

In the internet age, information is free and easily accessible for all users. The Internet has made life easy and simple, but this comes with a cost. If information is to be shared and available freely, it needs to be made public and thus privacy is jeopardized. Privacy is not a new concept but has been in existence before the era of the current telecommunication networks and technologies. Privacy is a natural action or reaction of individuals as one of their rights in public. However with the advent of the new technologies any and every information is made available. In this paper, we intend to show that privacy has been jeopardized because of these emerging technologies particularly networking advancements. Although there are different perspectives to privacy, we take the stand from the user perspective and argue that the privacy of the individual and so the community at large is being breached. We provide instances where networking technology has intruded into people's life and thereby justify the claim. We also provide evidences to show that privacy has been jeopardized and if people were to continue using networking technologies then there is no way that this process can be reversed.

1 Introduction

Privacy is important to people. People have the right to protect their identity, keep their personal space, and still be connected to the world in ways that they wish to. However, humans are social beings. We are interdependent on each other. Different groups of people are experts in different skill sets and we collaborate with each other to raise our total efficiency. In recent years, progress in technology has made this collaboration so much more efficient than before. Easy sharing of information like never before has made inroads in the kind of services that can be provided to make people's time more productive. In order to avail these services, one has to provide information that may reveal personal details, and in doing so one has to sacrifice his privacy. Even though this information has to be parted with several years ago, the ability for the service providers to misuse this information was very limited but in today's world, where social security numbers identify your credit history, driving history etc and your date of birth and mother's maiden name identifies you to call center representatives, information can be shared and misused very easily. This is the root cause for all privacy concerns today.

In this paper, we take the stance that loss of privacy is inevitable with the continued use of technology. We indicate examples where service providers gather private information of their customers and thereby support our claim.

There are different opinions which may suggest that privacy is not lost or can be restored. In this paper, we also indicate why this is not true and indicate in our example that this is the case.

2 Stakeholders

In this realm of discussion, there are two main parties involved.

The first party is the person who provides personal information to use some service. He is the victim of loss of privacy.

The other party is the service provider which uses the information which the customer gives. Service providers gather information to provide some service of value to the customer that makes his life easier.

3 Our Position

If things need to be automated by external entities to make life simpler, responsibility must be handed over to it. For this entity to carry out the job effectively, it has to be trusted and given the information it needs to perform the tasks effectively. Many times, this information that needs to be parted with is related to personal identity. Hence misuse of personal information is always possible and inevitable.

For example, in order to keep a home secure it may be efficient to hand over to a security provider who is an expert in that skill, the responsibility to protect the home. To do this effectively, the provider may gather information of the home, the occupants, their entry and exit patterns, identity of their friends and relatives and so on. They may need to install security cameras, perhaps to identify unknown persons through face recognition. All this information that needs to be handed over for effective service causes a breach of privacy.

Service providers will continue to need the information to keep up their quality of service. We think that this transfer of information is irreversible because:

- The transfer has already occurred in many cases as we cite examples in later sections of this paper. Information already known cannot be made unknown now. Voiding this information is possible (perhaps by changing one's life completely) but this comes at very high price.
- Customers will continue to seek for automation, personalization and customization to make their life more efficient. They will need to impart personal information to obtain this.

4 Evidence

In this section we present some real world scenarios which corroborate our statement that usage of technology has indeed resulted in loss of privacy and that this change is irreversible. We list few of the networking technologies that people use in their day to day lives but because of which people's privacy is being lost.

4.1 Internet

The Internet is a global system of interconnected computer networks that interchange data by packet switching using the standardized Internet Protocol Suite. It is a "network of networks" that consists of millions of private and public, academic, business, and government networks of local to global scope. Every user is connected to the world through the Internet. Every application on the Internet has the ability to keep track of information regarding the user i.e. his search history, his likes, dislikes, products that he purchased online etc. This information is private to the user and by gaining access to this information privacy is affected. For example Google has the concept of personalized web search by which it provides better search results to the user by combining information about the user's

web history. But for availing this service user needs to grant Google permission to track their searches.

When a user connects to the Internet, using networking technologies the user's IP address and through that his location information can be tracked. This might provide access of the user's computer to the outside world.

4.2 Mobile Technology

Mobile phones have come a long way since the early days of the 1980s when they were the size of a brick and weighed almost as much. As wireless cell phone use increases around the globe, the old CDMA and TDMA standards are being replaced with GSM/GPS. The GPS technology can be used to determine the location of the mobile user and can be used for a variety of applications. Though this technology was developed to provide more efficient services to the user, the location information which is used is accessible to the service provider. All the calls that one makes from his mobile phone, all the calls that he receives and details about each call like duration, contact information are maintained in a database by the service provider. With the advent of GPS in cell phones now, it is also possible to precisely locate and track the user.

As we have indicated many times in this paper, it is not necessary that the service provider will use this information against this user; however it still remains accessible and is being tracked. So it is a breach of privacy.

4.3 Snoop Server

A snoop server is a server that uses a packet sniffer program to capture network traffic for analysis. This technique is used in the business environment to identify security risks and/or to monitor employees' activities (such as Web sites visited). A snoop program puts network interfaces into promiscuous mode. This technique when misused can enable complete tracking of one's activities. Everything that one does can be monitored and maintained as history of activities.

4.4 Phishing

Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication .Though this is concerned with the security of the network, if there is a breach in the security the user information is made available to the attacker which amounts to violation of privacy.

4.5 Web Conferencing Tools

Web conferencing is used to conduct live meetings or presentations over the Internet. In a web conference, each participant sits at his or her own computer and is connected to other participants via the internet. Many web conferencing tools are available today and all of these make meetings and discussions convenient. However they also have a few disadvantages. When a user joins a web conference, then his computer is accessible by people participating in the conference through the remote desktop access. The user opens his desktop to the

outside world, so anybody who is part of the conference can gain control over the user's desktop and hence all information in his computer is vulnerable and open to the world.

4.6 Credit Cards & E-Business

Not too long ago, one had to carry with him dollar bills to make sure he can purchase what he wants at will. This mode of purchase did not leave traces behind because it is more difficult to track people from dollar bills.

Today, credit cards have made common man's life so much easier. It offers buying power with just a card in the wallet. The credit card in addition, offers security from it being lost or stolen. However, with its prevalent use, every purchase one makes is stored in digital format and can be traced back. Every little activity starting from purchase of groceries, borrowing of books and dvds, purchase of travel tickets, buying gas leave traces behind and gives the outside world the ability to know pretty much everything about a person. Just the history of credit card bills are enough to determine one's location, reading habits, hobbies, daily commuting patterns, travel plans, interests, internet shopping habits. Many users of this convenience are aware of the threat this technology poses, but tend to ignore the implications in order to enjoy the comfort.

4.7 Data Mining and Pattern Recognition

With the constant improvement in processing power, data processing is becoming cheaper by the day. Mining valuable information about customers is becoming a norm in today's business. By doing day-to-day business electronically, customers provide data to business. This information can be mined using various algorithms by businesses to discover specific audiences that fit their match in order to advertise their products more efficiently. Pattern recognition algorithms can be used to predict future behavior based on information from historical patterns. For example, Google places advertisements in emails that match their interests and relevance. This is indeed a breach of privacy for those who do not wish to be targets of such advertisements, but would like to use GMail.

5 Opposing Positions

Our stance that privacy is lost could be opposed in a few ways. In this section, we address some of the rebuttals that oppose our stance.

The first claim is the statement that privacy is not really dead. The reality is that total privacy is never possible in today's world. If one really wants total privacy, one has to live in disconnected from the rest of world to a large extent. He may have to sacrifice a lot of the conveniences that technology offers.

The other claim is that if at all privacy is lost, it is actually possible to restore it. Storage in digital format is unlike storage on paper. A paper can be destroyed easily, is less accessible and the ability to replicate information in this format is more difficult. However digital information is easier to replicate, share, hide and hence makes it much more difficult to destroy it without traces. For example, you may delete an email from your inbox, but you can never be sure that it has really been destroyed and is no longer accessible to anyone. So much information today has already been stored

in digital format and with the advances in networking technologies this information can be easily transferred, shared and stored. One can never be sure that all this information can be destroyed, so privacy would be restored.

Yet another claim that some may make is that as long as the service provider does not misuse the private information gathered, all is fine. One may argue that privacy policy specified by service providers may protect the consumer by ensuring that it is not misused. However, the fact still remains that the personal information is no longer private and is accessible by service provider if needed. Irrespective of whether or not it is misused, the information is no longer with just its owner. It has leaked outside, and has the potential to be exposed and misused. A fact remains that a large fraction of users do not know the implications of giving away their personal information to the service providers, and another significant fraction give it away knowing the implications because they want to utilize the services.

6 Conclusion

As we have indicated in this paper, technology creates so many situations where good service is offered at the cost of giving away private information. We have cited applications that are used in day to day life because of which private information is exposed to the outside world. We have stated reasons why this process of giving away information is irreversible. We have also addressed opposing perspectives about privacy.
In conclusion, people cannot do without the comforts that the new technologies provide them, but they need to be cautious and aware of the implications of their actions.

7 References

[1] Privacy and Technology, The World and I, September 1990 and Telektronik January 1996 http://web.mit.edu/gtmarx/www/privantt.html
[2] Internet and Privacy, Meshal Al-Fadhli
[3] Privacy Isn't Dead, or At Least It Shouldn't Be: Latanya Sweeney http://www.sciam.com/article.cfm?id=privacy-isnt-dead&sc=WR_20070710
[4] The Death of Privacy , A. Michael Froomkin