Computer Ethics

Gilberto Sepúlveda - 1056050

Wednesday, June 15, 2011

Enschede, The Netherlands

UNIVERSITEIT TWENTE

Abstract

Privacy and Security

Hotel “De Frislandse” is a fictional company that asked us to design a system with particular characteristics that may have important ethical implications. During this essay we are going to examine the best approach to build a system while considering the Code of Ethics of Software Engineers for professional practices. In the meantime we will outline the ethical implications and responsibilities of the stakeholders. This system is merely hypothetical and this paper aims to build a simple yet solid ethical rationale taking into account different ethical theories and recommendations to have a system with ethical values that consider the concerns of the end-user, the client and the software designer.

Index

Introduction

De Frislandse is a hotel in the island of Frisland that is planning to build a major system in the island's hotels members of the De Frislandse franchise. It's objective is to provide a better costumer support to the tourists of the island. To accomplish such objective the hotel is planning to develop and deploy a system of both hardware and software that is compatible in selected stores and venues around the island. However, the planning for the system requires to clear major ethical hurdles because the island of Frisland is subject to European privacy regulations and such system would gather a significant amount of data from its users. Not to forget also the criticism that it could face by its users. It is clear that for this system to be authorized by the Frislandic government for deployment, there has to be a clear plan where the personal information of the Frisland's visitors is protected and properly managed to prevent misuse and moreover the construction of a value-sensitive Design system where it takes ethical implications and moral values into account.

The System

The franchise De Frislandse had an initial plan to build the system and the requirements were the following:

> *The system must to be able to register the guest's name, address, credit card, phone number, next-of-kin details, etc.*
>
> *Within the hotel it has to monitor the usage of the Minibar, paid-TV, Internet, Phone and hotel room door as detailed as possible. Including the products taken from the minibar, which TV channels were being watched, phone and internet usage, the logs of the door being opened/closed. The franchise wanted all this information to use it as an act of proof in case of attempted scams.*
>
> *A key card that should be able to be used to access to different venues around the island and as a secure payment method for various clubs, restaurants and car rentals. In addition to local transportation and touristic attractions. The card is supposed to facilitate the visitor life since it could be used as a payment method that would be added to a sort of hotel credit so the user would pay everything in one bill at the end of his stay in the island (guest pays when they pay the hotel bill).*
>
> *The system should enable returning guests to have a profile that allows the room and services to be customized on the basis of explicit requests, as well as wishes that are derived on the basis of the services they used in previous stays (e.g. mini bar selection, pre-programmed TV channels, etc.) In other words the system would remember the user's preferences.*
>
> *Frequent guests could receive bonus points for each stay, which are credited directly to their card to be used with any of the hotel of the franchise or partner services.*
>
> *All these details were going to be used in order to present the guest with one all-inclusive, specified bill at the end of their stay.*

Description of the System

Hardware: This system consists of a large database center hosted within the confines of the island nation of Frisland. Portable access ports around the stores and venues of the

island track and interact with a personal ID that the user holds at all times. The user of the system has a wearable card with an RFID chip in it to track all his movements within the confines of the island.

Software: All the portable access ports communicate with the central server which manages the whole system. The heart of the system is in the server so that all the following actions are being tracked:

Within the Franchise's Hotels:

- Items consumed in from the Minibar
- Paid-TV Channels
- Websites visited by the user in one of the hotel's free computers
- Phone calls made within one of the hotel's free local phone line including called numbers and possibly voice recordings. In addition to the logs of the calls.
- Logs of the door being opened and closed

Outside the Franchise's Hotels:

- Websites visited by the user in one of the hotel's associated internet cafes
- Car rentals made by the user with the Secure Payment System in all the associated car renters.
- Purchases made by the user with the Secure Payment System in all the associated stores.
- Restaurants bills payed by the user with the Secure Payment System in all the associated restaurants.
- Venues visited by the user if payments were made with the Secure Payment System in all the associated touristic attractions.

Additional information collected even before the user gets into the island:

- Personal information such as full name, permanent address, credit card information, phone number, passport information in case the user comes from a non-EU/EEA country.
- The personal information of the people accompanying the main visitor or the leader of the group. (e.g. The Father with his family)

Controversial practice

The system presents several concerns regarding privacy issues. Due to the fact that the system collects personal data and tracks almost every single transaction done within the island's hotels and associates; Users of the system may feel disempowered to control their own personal data including but not limited to their purchases, their contact information

and their whereabouts within the island. Furthermore the system could produce a feeling to the intimidation to its users therefore generating criticism and/or negative reviews which could potentially affect the flow of tourism to this highly tourism dependent island nation.

Examples of ethical problems

In the upcoming section I am going to explain two possible scenarios where the system could lead to an ethical problem. The problems that this system may present are not limited to this scenarios only but those are merely an example of why the system could be controversial or subject of criticism in some cases.

Scenario 1: A politician

A congress of representatives of European countries will be held in Frisland with the objective of finding common grounds on several topics. Some of those representatives have visited Frisland before and the franchise De Frislandse holds almost a complete monopoly of the hotel industry in the island. It is therefore not difficult to be a repeated visitor if you hold a political position in an European country. One of those representatives was involved in a scandal earlier when he was seeking an important position in office. It's presumed that he was having a repeated affair with a woman in the island. Back in his country he is known for having an outstanding reputation among his constituents and if any evidence that could point out that he was in fact having an affair which he allegedly denied, his political career would be undermined if not completely finished.

Scenario 1: Consequences

While the politician may be doing a controversial and amoral practice at least according to western tradition, it is not the system nor the hotel/franchise responsibility to judge whether or not the politician should or shouldn't be doing that on the first place. The job of the system is to serve its users while keeping their personal logs safe. However the information it collects is highly sensitive and may be used as evidence that the politician was in fact having an affair.

If a scandal were to break out in the politician's home country those records would be highly valuable leaving the franchise De Frislandse in an uncomfortable position were it has to decide on either the listen to the demands from the politician's home country's political organizations and revealing his records (completely or to a degree) and avoid a popular boycott from the tourists of the politician's home country or take the infamous position of keeping the politician's private life secret and face the likely backlash.

Both positions would damage the reputation of De Frislandse, one because it revealed personal records and the second one because De Frislandse would not listen to the public demands from the politician's home country therefore resulting in a boycott against the franchise.

The franchise could have legitimate economical and ethical reasons to reveal the politician's records while having equally legitimate ethical and reputation motivations to do the opposite.
Furthermore the franchise may be forced to reveal the personal logs of the politician if a higher authority such as the Frislandic or European court orders it. Even without a court order, the franchise may decide to reveal the politician's record if the Frislandic government applies pressure on it or the reputation of the franchise has the risk to get damaged.

Ethical Problems

The main ethical problem that the system presents is that the system left the company in an uncomfortable position where it has to decide to satisfy the public and reveal the personal records of his guest while ignoring the user's concern or retain the information gathered and ignore the public concern.

Act Utilitarianism: From a act utilitarian point of view, the franchise should reveal the personal logs of the politician at least to either confirm or deny that the politician was in fact having an affair in Frisland and point at the evidence. This will make the most people happy since they will get what they are looking for and if the politician was in fact lying to the public, then the public can decide to judge him and trow him out of office or otherwise. What's good is that the the most people are happy and not angry and what is right is that the people know who is representing them so the majority can archive the greatest happiness.

Rule Utilitarianism: In Rule Utilitarianism what's good is what makes most people happy of course within the scope of the rules.If it's legal and makes the majority happy that alone gives justification to the franchise to reveal the politician's records. On the other hand what's right is that people know who is representing them, after all he is a public figure. Moreover there is no rule preventing the franchise from reveling his personal logs and people who have been accompanying him as long as highly personal information such as his passport number, credit card or so stays private. In both rule utilitarianism and act utilitarianism as long as the consequences are positive (which is people making a conscious decision about who is representing them), the act of disclosing his logs can be justified. This holds true specially if the politician happens to be conservative and/or have a strong religious affiliation where maintaining a monogamous and faithful relationship is a dogma and can't ever be broken although in practice (at least in American politics some high profile conservative figures demonstrate the opposite, however that's a discussion for another topic. (Rader, 2011)) One could argue that what would ultimately make the most people happy is to reveal the politician's personal logs but then we must apply the concept of universality. If it's good to reveal this politician's logs, should it be alright to reveal any others person logs if this other is having an extramarital affair as well?. Maybe,

Then De Frislandse would be a trap for anyone who goes to the island to have an extramarital affair, and this is hardly a good sales point.

Deontology: From a deontological point of view; the franchise has the responsibility to fulfill its duty as a company who keeps the privacy of its users. The politician trusted the franchise to manage his personal information so it's now the franchise turn to fulfill the politician's expectations and respond in an adequate way. Even though it may be right to reveal his records since he is a public figure, it's is not right for the franchise to decide on that, instead the franchise should leave it to the courts (or whistleblowers) if a case is ever made. After all the fact that the politician is having an affair with another woman other than his wife is not really a public concern. Unless of course the politician builds his political base around a theme advocating for conservative values and monogamy,.Then is when it becomes a public concern, and then is where part of his private life becomes public, last but not least then is when the franchise is justified to reveal his personal records. As for what is good; it's good to maintain a high and honest "breed" of politicians that represent the values of their community with high ethical standards. However if we are going to talk about deontology it's worth taking into account the concept of categorical imperative and its two maxims:

1. The three stakeholders involved in this issue are the franchise, the politician and his constituents. The politician is not acting right at least according to his constituents. The franchise would do the "right" action if they were to reveal the politician's records since what he is doing is not right and he is a public figure ergo subject of special scrutiny by the public. But if the politician was a person significant to the hotel, let's say someone who has a large amount of stocks or political influence over the franchise, the situation would most likely not be the same and the franchise would not follow suit with the previous statement of revealing this records making this case not universal. Not all politicians/clients are equal to the franchise.
2. The right conduct of the franchise is defined as archiving its objective without using anyone as means but as an end. The franchise is putting the company's reputation and costumers demand as an end, specially if the costumers tend to belong to an influential group of people. To archive this group's demand, the franchise needs to use the politician as a mean since it is his personal information what is going to be revealed.

Ethical and Legal responsibilities

The legal responsibilities of De Frislandse's system must be to ensure the users privacy unless a competent authority demands a disclosure of the records. De Frislandse has however the responsibility to abide the rules and only the competent authority should be able to overrule the privacy protection practice of the franchise. De Frislandse is responsible of informing the user what is being tracked in a clear manner and the reason why it is being tracked.

Prevention or Reduction of Damage

It's important to consider that technology is not morally neutral. For this is important to design a system that empowers the user to select what is to be shared and what is not. An option of storing information as anonymous and an always available option to opt-out from the system while enjoying some if not all of its benefits (this last one may run against the interest of the client) are two possible solutions to the problem.

Scenario 2: A Security Hole

The franchise De Frislandse has been collecting and storing personal information of its users for a while. All this information is systematically stored and labeled in its servers within the island. De Frislandse spends several thousands of Euros to keep its server up to date against any security treat, after all the franchise collects highly valuable information from its users.

It just happens that a group of cyber-criminals presumably based in China targeted several American and European tourism companies. Their attack was highly sophisticated and one of the companies who suffered an information leak was De Frislandse. The hackers accessed the unencrypted information and stole hundreds of credit card numbers along with their names and other personal data such as accompanying visitors and passport numbers. This could only mean devastating news to the franchise and they decide to notify its users immediately.

De Frislandse in a press release informed the local newspapers that the data of the visitors that was compromised belongs to people who made use of the system 3 years ago. The reason of this failure was due to the fact that the data of these non-frequent visitors was transferred to a less secure and cheaper server with an outdated security software. The press secretary of De Frislandse revealed in a statement that the company was struggling to pay for the more expensive and secure servers due to the low turnout of visitors because of the latest economic recession which heavily affected Frisland's tourism industry.

Scenario 2: Consequences

The user and user's guests personal data has been compromised. Highly confidential information such as passport numbers, credit card information and address would be now in the wrong hands.

This information may be used to falsify the user's identity online in addition to produce fraudulent economical transactions that will ultimately affect the end user and ultimately damaging the reputation and credibility of De Frislandse.

Ethical Problems

This is a classical mistake that has happened to some companies on real life. Information thieves are everywhere and they are practically untraceable. The internet has brought us together but has also brought new concerns to consider.

Act Utilitarianism: The franchise collects this information to better serve its users and be up to the trends. Collecting information for statistical purposes can give a better user experience to the users therefore a better or less worrying vacation time while they are in the hotel. The franchise is in every right to store the information to be able to facilitate the lives of its users while giving them a more comforting user experience. However the franchise did not do right by moving the information of its old users to a less secure and cheaper server and while it may be driving costs down to provide affordable vacation packages to its users even on difficult economical times it's potentially exposing its reputation and its users information which may end up in a disastrous scandal.

Rule Utilitarianism: As with act utilitarianism the franchise worked within the rules and it was just unfortunate enough to be targeted by a third party. The problem is that while the franchise may be giving a great costumer experience while its users are in the island, it may bring a painful side-effects once the costumers leave the island. Both act and rule utilitarianism consider the concept of universality which means that if every company did the same practice of storing information of former users in less secure but cheaper servers to drive costs down and offer better prices instead; The user information would constantly be under threat and if a massive information breach happened like it is in this case, it's most likely that the users won't ever trust the franchise anymore and probably most of them would feel insecure and unhappy regardless of how well was their time during their vacations in the island or how cheap are the packages that the franchise offers.

Deontology: The franchise did not do right by moving its information to a less secure and cheaper server. It is their duty as information collectors to ensure that the information of their users is safe and secure. If they can't accomplish such duty then they shouldn't even collect the information on the first place. It does not matter if the franchise refunds its users or gives them any reward, the franchise did wrong to retain the information and move it to a less secure server rather than getting rid of the no longer used information. It's worth defining the two Kant's formulations for deontology in this section:

1. The franchise is clearly not thinking about the consequences created by this practice. If every major database were to put old users into less secure servers, users would be found themselves in constant threat making a less secure world where users would need to think more about what information is being gathered. This would likely discourage companies from gathering data since it could prove to be unpopular among costumers therefore making companies less likely to be able to build product with a high value on costumer experience since the data would be inaccessible or difficult to gather.

2. People are being used as means to save some money and prevent the franchise to go bankrupt. In this sense the franchise is doing a clear and transparent moral wrong.

Ethical and Legal responsibilities

Both the perpetrators and the franchise De Frislandse is liable for any misuse of the information that was breached. At the same time the people who advised to move the user information to a less secure server even if temporary have an ethical, moral and legal responsibility. The user in this case does not bear any responsibility and it's merely the victim of an act that he could have not known or prevented. The system pushes the user to opt-in the system making the franchise even more responsible for pushing its users to opt-in while mismanaging their information and making the software designer morally responsible if it did not advice the company that this consequence could potentially happen if users are forced to opt-in. Of course it's worth to consider that the system designer is always expecting that its client is updated and the users to trust its client.

Prevention or Reduction of damage

De Frislandse could have reduced the impact of this damage by ensuring complete deletion of the information stored in its servers by setting a time frame were the information stored is completely deleted and/or anonymized for statistical purposes. The franchise faces the classical problem of holes in its security structure which may exist with or without the knowledge of the franchise.

On May 2011, a group of hackers broke into the security system of Sony's Play Station user database, stealing passwords and other personal information along with credit card details. (Cohen, 2011) This security breach has damaged the reputation of Sony among players permanently. Sony was criticized for not even encrypting the information which happens to be a basic practice that all databases that interact with online users must have by default. Encrypted Credit Card information could have gotten stolen as well but Sony did not confirm on this. ("Sony faces legal," 2011)

The lessons from Sony could be applied for this case. The Internet is not a 100% secure network, it's architecture makes this impossible. However there are certain measures that all databases on the internet could take such as never storing names and payment information and addresses together in one single database. Ensure that a proper encryption is applied to all the information and schedule the deletion of this information after a determined amount of time, IP addresses should be regarded as highly sensitive information because they are capable of pointing the source of the information. For not sensitive information that can be used as statistical data should be anonymized leaving absolutely no trace to the author or generator of the information was in the island.

Although it may seem impossible nowadays, maintaining an offline database could be another feasible option. In the case of De Frislandse where the servers are located within the island, doing such thing is an obvious step for a higher degree of security. However

this tends to be difficult to archive since more and more information is being stored in the cloud because of its convenience but also because of its global reach.

Accountability and Responsibilities

To prevent any failure both the system designer and the franchise must consider that any liable responsibility regardless if it's casual or by fault; it's shared by both the system designer and the client (De Frislandse). Fortunately in the case of this system there is no apparent way the system can physically harm the end user. Nevertheless the three parties have their own responsibility to ensure no problems will ever be produced.

System Designer: From the system designer side the designer must be accountable for any system failure that may put at risk the user's wellbeing. The system designer is responsible to asses the client and guide him to choose the best ethical practices possible. The system designer is liable if the system does not follow the specifications of the client or harms the end user. The system designer has the moral responsibility to comply with both the end user (first) and the client (second) according to the software engineering code of ethics. (ACM & IEEE-CS) The system designer shares the casual responsibility with the client unless the software was misused and assuming the software comes without deficiency. The system designer has the responsibility to blow the whistle if the system poses a serious treat to the end user or the whole public, and the client is negligent to change the system to address the issue. Some barriers such as many people from different places designing components of the system may pose hurdles to identify who is the exact culprit. (Coleman & Gwen, 2004)

Client (producer): The client on the other hand is the public face, the one who has a direct relationship with the user (end-client). The client requires to consider the ethical implications and recommendations provided by the system designer. Since the producer is the one that provides the economic means for the building of the system, it is the producer the one that has the most power to make significant decisions regarding how the system is going to behave and what embedded values should the system have in a general context. However the system designer will always have the ability to define the details of the system in a more specific way than what the producer can do. The client is probably the stakeholder with most of the legal responsibilities, specifically if the software is being knowingly and/or purposefully misused. Some barriers to identify the responsibility may arise specially if there is no clear understanding of who is in charge of what responsibility. (Coleman & Gwen, 2004) The client as a company is unable to have any moral responsibility since a company is not a person, however individuals within the company have the moral responsibility of providing usable and reasonable products to the end-user by vetoing anything that can pose a treat to the end user. The client has a chance to have the casual responsibility if it ignores the ethical recommendations of the system designer and demonstrates negligence towards the end-user needs.

End User: The end user is responsible to use the software designed to his use in an appropriate manner, according to the instructions for what the software was designed for. If the user is doing intentional misuse of the software then the producer and the system designer can't be held accountable for any failure that the system may cause. The end-user has the moral responsibility of using the system as it is intended if comprehensible knowledge is provided. The user is liable if he is knowingly misusing the system to cause harm to someone or something else (a company or group). Some barriers such as "blaming the computer" for the incident or assuming that the system is ethically neutral can make the user not to be able to see that he is not responsible for many of the negative effects caused by the system. (Coleman & Gwen, 2004)

System (Computer): As for today the system or the computers can't ever be held liable for anything. While systems aren't necessarily morally neutral they can't be held morally responsible because there is no intention in them. Softwares are machines composed of words and they have a clear function. If the function is flawed it's because of the author of the code and in some cases the end user can also be the one who is at fault. Friedman and Kahn argue that instead of trying to find liability on the computer systems we should design the systems in a way that they make it obvious that the responsibility does not rely on the system. (Friedman, & Kahn, 1992) At the same time since computer systems are not suitable to be accountable for responsibility they are also not suited to make judgements. (Ladd, 1989)

At the end, both the designer and producer have a significant share of responsibility and the two groups should be held accountable for their decisions and practices if a fatal event were to happen. This however does not frees the end-user from the responsibility of being responsible if he/she misused the software or tool. If every party involved follows suit then the system can reach a balance where every party can respond properly without fearing of being abused by the other. Just as Dr. Nissenbaum once wrote in her article Computing and Accountability "accountability server as a powerful tool for bringing about better practices, and consequently more reliable and trustworthy systems" (Nissenbaum, 1994)

Privacy

Privacy as described by Lucas Introna is a complex concept to define because what is considered private in one culture may be considered part of the public domain in another. (Introna, 1997) Even within similar cultures this can prove to be true. While a representative having an extramarital affair can be a scandal in the United States, it may not be as scandalous for a country like the Netherlands or Sweden. This is probably due to the perspective of what the private realm of a person constitutes as opposed to the public

one in addition to the expectations that the public sets over a public representative's private life.

Introna divides privacy into three different categories which are useful for the sake of this paper. Introna defines privacy as:

a) The lack of access to a person or his/her "personal realm" (Introna, 1997), or as Samuel Warren and Louis Brandeis put it "the right to be let alone" (Warren, & Brandeis, 1890).
b) The "control over personal information" (Fried, 1968) [by the information owner or user for the sake of this paper]
c) The "immunity [freedom] from the judgement and scrutiny of others" (Johnson, 1989)

Everyone has a public and private life, or at least everyone in the western tradition. What may constitute part of the private realm is a subject of debate. Every society has its own definition of what constitutes the private realm and when a person has to give up some of that information to the public realm. In the American tradition for instance, it is always for a politician to reveal his or her family life. The higher the position the politician is seeking the higher the public will scrutinize his or her private life.

Why is privacy Important

Metaphorically speaking; privacy is important because privacy are the walls, windows and doors of a house which divide the outside from the inside. In an individualistic society such as ours, privacy is one of the strongest characteristics that define an individual or the unit of a society. Privacy defines the personal boundaries of what constitutes the private life of a person versus the public life. In some cultures the privacy may be set not in the individual but on the family in a more communitarian approach.

Fried defines privacy as "the moral capital" or the currency required for the formation and stability of an intimate relationship. (Fried, 1968)

Where is the system violating the privacy of its users

Technically speaking the system does not violate the privacy of its users if the users agreed on the first place to such activity (although the user may not even know what he or she is agreeing on). If the user wants to be able to use all the benefits that the system brings, they need to opt-in and give consent to the system to collect all this sensitive information. However the system contains embedded values that are quite obvious. The system does not allow the user to opt-out at any time once the user has opted-in. The system does not provide an anonymous option where all the specific information collected by the system of the user is instantly deleted or deleted after his departure. The only option that the franchise gives to its users is to either opt-in and enjoy the benefits of the system or opt-out and very likely pay a higher price since the user would be unaware of discounts and offers. In addition to that, the franchise controls almost all the hotels in the

island giving little to no real alternative option to the visitors. Not to mention that many business both within and outside the franchise's hotels are linked and provide information to the system making it almost impossible to avoid the system. The system is designed to make people to want to opt-in into the tracking program which brings benefits to the end user at a not so obvious cost.

Why is data mining Important

Data mining the "process of discovering pattern in data" provides an opportunity for the company to know the demographics of its guests better. (Tavani, 1999) Unlike data gathering, data mining does not provide information of an individual but it does provide information of individuals alike. The information gathered by this process should not be taken as a fact unlike the information retrieved from data gathering techniques. The franchise has legitimate reasons to mine data from its users for statistical purposes, but it would be wrong for the franchise to assume that this data represents an absolute value or a fact. If the user is able to show that the data gathered from data mining techniques does not represent him or her, then the franchise must dismiss that data in the user. The franchise can use data mining techniques to adjust the price of its hotels to different demographics, and promote itself in the desired markets to increase the likeness of potential visitors to visit the island in one of the many hotels of the franchise. Data mining information should be always anonymized and never be considered as an absolute value or used if it will affect the end-user interest. If the franchise believes it can't hold to those expectations then it should not practice data-mining.

Storage and Encryption

System tendency to push users to opt-in

The system as mentioned earlier, contains embedded values and it's designed to encourage its users to opt-in and so the users give away their information to the system. While the system does ask for consent from its users; The users opt-in because of the monetary benefits that they get from the system. However this does not need to happen, the system can still collect data and anonymize it for statistical purposes. The system can give the option to the user to opt-out whenever he wants and the system can provide a completely anonymous option in the same fashion that modern browsers do. Furthermore to prevent the user data from being compromised the system should be able to delete the stored data of the users who opted-in after a reasonable amount of time, preferably based on the time that it takes for an average visitor to revisit the island.

Storing information and Information Encryption

The system should not ever store the user names and credit card numbers and addresses in the same database and should encrypt all the highly sensitive data such as names of visitors and guests of visitors, passport numbers, credit card information, addresses, etc.

Otherwise the De Frislandse has the risk to face the same fate as Sony when its user database of Playstation users got compromised. (Murphy, 2011)
As mentioned earlier, the system should not store highly sensitive information such as names and credit card numbers in the same database. If the system ever gets compromised then only a part of it would get compromised. The franchise De Frislandse has a legitimate reason to store all this personal data since it needs to charge the fees and know who is staying in its hotels however if they are going to take the task to do so they should always fragment the data so it can't be collected all from one place.
Nowadays it's extremely important to expect the worst possible scenario. Just as the internet has brought benefits, it has brought new concerns to consider. Criminals are practically untraceable, stealing information in massive amounts hasn't ever been so easy as it is today. As more information gets stored in the could there are more dangers to consider.

As for the not necessarily personal data such as logs of the door opening in which privacy can be lost but shouldn't ever be violated the system should link the data to an anonymous character or number that cannot lead to the original user. Unless the user explicitly agrees to opt-in and allow his records get linked to his name. Furthermore the system should provide the user an easy, obvious and intuitive interface to control exactly what can be tracked and what cannot therefore empowering the user to control his information. Giving the power to the user to decide can clear any ethical hurdle regarding privacy for De Frislandse as long as the interface where this is presented is easy to use, intuitive, accessible and understandable. The user should be able to alter his settings at any moment, at any time and get assistance at any time. De Frislandse is entitled to assists its users whenever they find some hurdle such as a disability or age. It's important to consider that while the interface can be presented online (although preferable if it's within an intranet network for a higher standard of security) some people do not feel comfortable using a computer, therefore an phone option should always be available for this matter.

Conclusion

Many interesting concepts of computer systems and its ethical implications have been explored in this paper. There are some modifications that can be done in the architecture of the system to prevent a potential leak or attack to the database containing the user's information therefore decreasing the likelihood of a disastrous information leak.

Privacy is relevant to everyone, even though it's hard to define. In some cases privacy plays a central role in the characteristics of the system that certain company has to offer. For example; Facebook initially offered it's users to be connected to people who are relevant to the user and yet maintain a high degree of privacy. However over time Facebook has done some controversial moves; exposing the personal information of its

users to third parties and the web in general (potentially providing more information to the companies who practice data-mining techniques) as Matt McKeon explains in his graph of the Evolution of Privacy on Facebook. (McKeon, 2011) Privacy is in many occasions the competitive advantage or the feature that one company offers over the other. In some cases is not privacy at all but the simple perception on whether or not the company handling the information has a positive or negative history regarding the management of privacy of its users. For instance Facebook was involved in a scandal were it hired a PR firm to promote a smear campaign against Google's privacy practices. (Carbonell, 2011) Which is itself ironic because both companies have been in multiple occasions in privacy-related scandals.

About the Author

Gilberto Sepulveda is a student of Human Media Interaction at the University of Twente who has a deep interest in human rights (specifically minority rights), visual design and technology and politics.

Bibliography

- ACM, , & IEEE-CS, . (n.d.). *Software engineering code of ethics and professional practice*. Retrieved from http://www.acm.org/about/se-code
- Carbonell, R. (2011). Facebook's hiring of pr firm to smear google read more at suite101: facebook's hiring of pr firm to smear google | suite101.com http://www.suite101.com/content/facebooks-hiring-of-pr-firm-to-smear-google-a372261#ixzz1qvwol2zu. *suite101*, Retrieved from http://www.suite101.com/content/facebooks-hiring-of-pr-firm-to-smear-google-a372261
- Cohen, P. (2011). Sony security hole exposes another 24.6 million accounts. ZDNet, Retrieved from http://www.zdnet.com/blog/gamification/sony-security-hole-exposes-another-246-million-accounts/361
- Coleman, Kari Gwen. (2004). Computing and Moral Responsibility. *Stanford encyclopedia of philososphy*. Retrieved July 1, 2011, from http://plato.stanford.edu/archives/spr2010/entries/computing-responsibility/
- Fried, C. (1968). Privacy. (pp. 475–493). Yale Law Journal.
- Friedman, B, & Kahn, P. (1992). Human agency and responsible computing: implications of computer system design. Manuscript submitted for publication, Millis College and University of Houston, Oakland, CA and Houston, TX, United States. Retrieved from http://www.sciencedirect.com/science?_ob=MImg&_imagekey=B6V0N-48XVCT0-7T-1&_cdi=5651&_user=499905&_pii=016412129290075U&_origin=&_coverDate=01%2F31%2F1992&_sk=999829998&view=c&wchp=dGLbVzW-zSkWb&md5=44987b9a6bf604a495cde1a0ea8f6c36&ie=/sdarticle.pdf
- Nissenbaum, H. (1994). Computing and accountability. Manuscript submitted for publication, Center of Human Values, Princeton University, Princeton, NJ, United States. Retrieved from http://delivery.acm.org/10.1145/180000/175228/p72-nissenbaum.pdf?ip=130.89.172.88&CFID=30755315&CFTOKEN=57909010&__acm__=1308946945_74d9cd9a2a1712ee63de5b10f3a65a21
- Introna, L.D. (1997). *Privacy and the computer: why we need privacy in the information society*. Cambridge, MA, United States: Blackwell Publishers.
- Johnson, J. L. (1989). Privacy and Judgement of Others. (pp. 157-168). The Journal of Value Inquiry.
- Ladd, J. (1989). Computers and Moral Responsibility, in The Information Web: Ethical and Social Implications of Computer Networking, C. Gould (ed.), Boulder: Westview Press.
- McKeon, M. (2011, July 01). *The evolution of privacy on facebook*. Retrieved from http://www.mattmckeon.com/facebook-privacy/
- Murphy, D. (2011). Sony europe hacked: 150 accounts compromised. PCMag, Retrieved from http://www.pcmag.com/article2/0,2817,2386414,00.asp

- Rader, E. (2011). Gop not the family values party.Pride Source, Retrieved from http://www.pridesource.com/article.html?article=47715
- Sony faces legal action over attack on playstation network. (2011). BBC News, Retrieved from http://www.bbc.co.uk/news/technology-13192359
- Tavani, H. (1999). Informational privacy, data mining, and the internet. *Ethics and information technology*(pp. 137-145). Nashua, NH, United States: Khuwer Academic Publishers.
- Warren, S.D., & Brandeis, L.D. (1890). The right to privacy [Vol.IV, No.5]. Retrieved from http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html