University of Victoria, Software Engineering

Case Study 9: Privacy

Jordan Ell
V00660306

March 20, 2013

1 Question One

Q: What aspects of these new security measures raise privacy concerns? Are there any specific to the security cameras or the ID scanning systems?

A: There are three aspects of these new security measures which raise privacy conerns. The first is the issue of being video taped outside of the night club. Here, the customers of the night club are in a public place where they need to be told that they are being video taped when possible. This violates the privacy concern of consent. If a user does not wish to be filmed, fearing their identity be know for whatever reasons, they should have reasonable ability to avoid it. The second issue is that of the photo ID card swiping to store personal information such as race, age, nationality, etc. Here again is the violation of consent. If a customer of the bar does not wish to hand over that type of personal information to the bar owners, he or she should not have to. These two types of privacy concern are specific to the security cameras and the ID scanning that Vivian wishes to put into place. However, there is a larger concern to privacy here that Vivian intends to violate, and that is about the distribution of personal information collected by the bar. Vivian should not be able to (with not consent) collect and then sell information about the customers to third party companies for a profit. This distribution violates a customers privacy because unknowingly their information has been passed into a number of hands without their knowledge. Finally, the distribution of customer personal information, freely, to social networking sites. Not only is this a gross misuse of personal information collected by the bar owners but now that information is availible to be distributed further

by third party participants with no reprocussions onto themselves. These are the major concerns with privacy and the new security system that Vivian intends to implement.

2 Question Two

Q: Which Act applied to this scenario? Based on what you know, what requirements of that Act will shape the way that Vivian can implement the new security system?

A: The Freedom of Information and Protection of Privacy Act (FOIPP) directly applies to this circumstance. FOIPP is designed so that public bodies such as the JBar night club are more accountable for their actions to the public. FOIPP provides right of access to records, limiting what can be stored on record, and gives people a right of access to their own information. More importantly, FOIPP says that when collecting information directly from an individual, the public body must provide a collection notice that informs of purpose, authority, and contact information. With this act in place, Vivian must can steps accordingly. Vivian must post notice outside of her night club that informs customers that they are being video taped and for the purpose of the video tape. Customers must as have some way of knowing what the information is being collected for and have the ability to access that information themselves. A second act that will have effect on Vivian's business is the Personal Information Protection Act (PIPA). This act states that explicit consent must be given by the customers to have their personal information collected in the proper circumstances. This will effect Vivian in the ID swiping. She will have to get consent from the customers to be able to swipe their photo IDs and be able to store the information.

3 Question Three

Q: What actions should Vivian take to ensure that the new system is complient with the privacy legislation?

A: Vivian should take both technical, legal, and procedural steps to ensure her new security system is complient with privacy legislation. The technical steps are as follows. Vivian needs to have a system in place, whether that be email, a website, or a phone hotline, that will be able to be used by customers to gain access to their own personal information that Vivian has stored. A second technical step is that she must ensure that her actual storage of information is secure. This could be anything from storing video camera logs on encrypted hard drives, to having a locked room where records are kept. The legal procedures that Vivian should take mostly are centered around notice and consent. Vivian should post signs in and outside her night club, wherever they are recording video of customers. These signs should also explain the purpose of the video recordings and and authorities that will have access to it such as police or third part marketing firms. Vivian should also require he staff to ask for consent while scanning photo IDs and should again explain the purpose and authorities with access. Finally,

Vivian should put into practise security procedures for the distribution of data she is collecting. Vivian should not be posting security camera footage to social networking websites with explicit consent of the patron to the night club.

4 Question Four

Q: Some of the information will be posted on a social networking site. How would this be problematic from a privacy perspective?

A: This is extremely problematic from both the notice and consent side of the privacy perspective. Customers, at this point, are unknowingly being filmed for their personal information (or having their photo IDs scanned). Also, consent was never given for the collection in the first place. Now, Vivian wants to take this illegally collected information and distribute it on the interest again without consent. The customers of the JBar have had their privacy breached now not only by once person, but by everyone on the internet able to see their information. This is a huge issue. What ever Vivian intendes to use the collected information for should be displayed to customers in some manor as they enter the bar. This is similar to how websites such as Facebook and Twitter have terms of use agreements before you can use their website. They outline exactly what they will be collecting and how they will be collecting it. More importantly they tell you how they will use the information once it is collected and who will have authorization to view that data. Physical environments should adapt the same policies as the internet. This is an almost backwards way of thinking, however, the internet does seem to get privacy right for the most part when money is involved.

5 Question Faive

Q: How do issues of security and privacy interact in vivian's case? In your opinion, what is the appropriate balance between security and privacy to be struck in circumstances like this?

A: In physical environments, such as the JBar, security and privacy often come as a trade off. The more security one has in the environment, often the more privacy one has to give up and vise versa. This trade off has become more prevalent as security functionality through technology continues to evolve. In order to keep her repair costs down from vandalism and her negative impact from media to a minimum, Vivian has to increase the security and personelle tracking at her bar. In my honest opnion, I think more privately owned businesses that are open to the public should adopt higher security standards through technology. We see this on the internet all the time. Facebook's terms of use agreement continues to evolve every year in order to protect itself from legal issues while keep customers informed of its data collecting policies. The key word here is customer. This applies to the real physical world as well. If you do not like Facebook's terms of use, then don't use it. If you don't like that a bar won't let you in without gathering

information about you, then don't go to that bar. It is all about consent. Private companies can install which ever security measures are needed as long as customers are aware of the freedoms they are giving up once they enter. If they do not want to give up said freedoms they can choose not to enter. These issues are a matter of people believing company services are a right not a privlege.