Info 3

Laboratory 1

Prof. Weber-Wulff

16.04.2020

ChungFan Tsai
(s0571269@htw-berlin.de)
Ba Tung Linh Pham
(s0571626@htw-berlin.de)
Florian Holzmann
(s0568263@htw-berlin.de)
Mohamed Amine Sallami
(s0565283@htw-berlin.de)
Pavel Tsvyatkov
(s0559632@htw-berlin.de)

Lab Exercise: Case 1. Sensitive Health Data

Questions 1 : Who are the actors in this scenario? There may be unnamed actors, and not all named actors are truly involved in the case.

- **Insurance Company Free & Easy** (The main actor behind Chris and Susan since they let their worker gain the access to a sensitive database "freely & easily")
- **The insured people of Free & Easy** (The victims, whose datas are controlled by Free & Easy)
- **Chris** (Main character here, who accidentally became a potential thief because she is received such a powerful tool from her company)
- **Chris's children** (Family members of the main character, they would play a small role here)
- **Susan** (Partner in crime of the main character)
- **Media/newspaper** (They are willing to buy informations without caring about the source)
- **Governments** (Same as Media/newspaper)
- **The other blackmailer** (Did they just save Chris and Susan from becoming thieves here? Or they are just Chris and Susan but came a bit earlier)
- **Ralph** (like insured people of Free & Easy, but he is the first victim who is "attacked" by Chris)
- **Ralph's new family** (Same as Ralph)

After we read through the case study, everyone shared their thoughts about the situation briefly and started discussing about the actors in this scenario. At first everyone mentioned **Chris and her children, Susan, Ralph and his family, and the insurance company**. Chris went out of her way and looked up her ex-husband's family policy and even printed out the details on a page. Later on together with Susan they were partners in crime, trying to find sensitive data and potentially sell it. Ralph and his new family, since sensitive information is revealed about them. The insurance company, which is also at fault here, because they gave Chris access to a sensitive database.

We discussed further and agreed that **the insured people of Free & Easy** are also actors in this scenario, since their data is controlled by Free & Easy, later in the text we can see that Chris and Susan found data about politicians, a singer and a movie star.

Governments, newspapers and other media are also potential actors, since they are the ones who are willing to buy sensitive information and use it.

Questions 2 :What are the ethical problems (not the legal problems) involved in this scenario?

We have together come up with some points that are ethical problems in our opinion:

- We all think that accessing peoples' private data without their permission would definitely be a serious ethical problem here.
- Using the company's data for non-professional reasons is also something that we should always avoid.
- Chris has also shared sensitive information with a 3rd party (Susan)
- Chris has saved company's datas on her personal device(USB), and also printed out the page on Ralph's new family.
- Chris and Susan have planned to sell datas, they have not done it yet but still, they thought and planned for it.
- Potentially injuring others, their property, reputation, or employment by false or malicious or negligent action or inaction.

There are also some points that we found in the codes of ethics, which pointed out the situation here.

Due to BCS:
Duty to Relevant Authority You shall: d. NOT disclose or authorise to be disclosed, or use for personal gain or to benefit a third party, confidential information except with the permission of your Relevant Authority, or as required by Legislation.

Due to ACM:

1.1 Contribute to society and human well-being.

1.2 Avoid harm to others.

1.3 Be honest and trustworthy.

1.7 Respect the privacy of others.

1.8 Honor confidentiality.

2.3 Know and respect existing laws pertaining to professional work.

Questions 3 : Since Chris and Susan destroyed the data before attempting anything, has any real harm been done?

With this question, we didn't all agree with each other. Some of us believed that since the plan hasn't been carried out, no harm was done, because what they think

the harm isn't tangible or physical. But some of us believed that the fact that the health information of Chris's ex-husband's family was already accessed by her, his privacy has already been harmed, and most of us agreed that the breach of privacy constitutes real harm.
Another victim of this situation is the company, even though this wasn't clearly stated in the case, we believe that most companies want to protect their tangible and intangible properties, including their customer information. And the simple fact that Chris allowed Susan access to those properties has harmed the company deeply. Just because they haven't taken any action to blackmail or leak the information this time, doesn't mean they won't try that again, or the information won't be further transmitted to other people or institutions.

Questions 4 : Is there a problem with Chris' children having access to her computer?

Basically, there is no real problem because they didn't have the password to access the data or the software that could access the data. And as mentioned above, she didn't save any data in her computer, but in a USB instead. It's also her own computer, not an asset from her company so there should be no rule of controlling that computer but only the software. Legally, it's ok for her children having access to her own computer. But despite the fact that her children are still pretty young (13-year-old boy and 8-year-old girl), there is always a potential harm that Chris forgets to log out her account after work/ saves her password automatically/ stored her company's data locally accidently/ virus/ etc… and it could lead to the data leakage. It should be under control by Chris while her children have access to her computer, or she should ask her boss for more information about that situation. It's always sensitive when her children use her computer which contains a huge amount of data, even it's her own computer. Let's just say it's ok for the legal aspect, but this kind of thing should always be avoided.

Questions 5 : Are there any side issues that need to be addressed?

At first we were quite unsure what side issues are there. But then we started to think, is the company really of no blame in this situation? Why would they let anyone access sensitive information from everyone with just one password? If we are the customers of this company, we would be extremely worried that our information would be abused and published. The company is for sure liable for giving a customer service personnel so much power. We think that the company is at fault for not having implemented a more secured system and thus put the customers' information in danger.

Another problem we found is that Chris was allowed to use her own computer and not a device from the company to work. The problem with this is, your personal/or even family computer can be accessed by someone else, and your personal use can lead to the computer getting hacked or infected by a virus. Not to mention once you

quit the job (or terminated), how can the company be sure that you don't have their information stored on your device. If you sell it second hand or to a recycling store, they might be able to access it and abuse it. Another side issue is that she printed out Ralph's details on paper, but we don't know what happens with the page after. The paper could potentially be found by Chris' children or if there is an investigation later.

We think that the company should at least have a record of which employee looked up which document and downloaded or printed them out. If possible, even providing the customers a confirmation code sent to them when they call in, so they can provide this code for the customer service to access their private information if needed.

Other minor issues which may be a bit unrelated, we weren't sure, but shouldn't the newspaper and the government being sold these private information confirm that the source is legal? Doesn't the media have their professional obligation to confirm the legitimacy of the content and the legality of the source? Of course we are all aware of the existence of some unethical media source. But we believe those who monetize off illegally obtained content should be strictly regulated and harshly punished.

Place yourself in a character, who knows about the situation(about what they were going to plan but did not do it actually). How should we handle the situation?

Fan: If I'm aware of this incident, I'd report this colleague (or even if I'm not an employee, I would still contact the company). I would even go as far to tell people not to get insured with Free & Easy. They might sue me for defamation or something like that, but letting a company carelessly manage people's sensitive information is definitely something that should be stopped and disclosed.

Linh: The problem here is not if Chris and Susan are guilty or not, if they are accused for what they have not actually done. I will have to report it for people's safety, for the customers of Free & Easy so that the company will be more aware of their security hole. The idea that Chris and Susan came up with will be on other people's minds anyways if the company can't control such a huge amount of information like this.

Pavel: In my opinion, this should definitely be reported as it is invasion of private information, which was used for non-professional needs and shared with a third party. I think the company should also be held accountable, because a new employee shouldn't have access to all the sensitive data of the company's customers.

Amine:I think there is no excuse for what Chris and Susan did. Even if for her it is information that concerns her indirectly since it is the father of her children, this will not justify the use of its power to access personal data of customers, and for that I will report what she did. I will also claim the company did not protect such information from its employees or even not be responsible in its recruitments. Finally, personal data is very private, it is the role of companies to protect their customers' privacy.

Florian: If I would know about this situation, I would report this situation to the company, to protect other customers from information fraud. There are some serious trust issues in the company.The company got a partial guilt to not have security features to prevent this breach of privacy by Chris.

Time Spent

We spent around 1hr reading over, discussing, and referring back to the folie in the lab. Then afterwards we each spent about 1 hour(2 hr if they are the ones writing up the answers) filling in the details we discussed.

Task Assignment

We had the discussion together during the lab. Everyone contributed some of his or her opinions. The answers to the questions were mostly done by Fan, Linh, and Pavel. But we all contributed our opinion as of how we would handle the situation.