Putra Business School

GSM 5170 Management Information System

Dr. Rusli Haji Abdullah

Lecture 9

Case Study 1: Sexting Now Almost Commonplace

Case Study 2: Sony Reels from Multiple Hacker Attacks

31st March 2014

Uma Devi Muniyandi: GM04926

Case Study 1: Sexting Now Almost Commonplace

1. ***Adult sexting is perfectly legal, as it is the sharing of sexually explicit content between two consenting adult. But what about teen sexting- should that be legal? If a 16 year old boy sends a sext to his 16 year old partner should that be considered child pornography? Why or why not?***

ANSWER

Sexting is the act of sending sexually explicit messages and/or photographs, primarily between mobile phones. The term was first popularized in the early 21st century, and is a portmanteau of sex and texting, where the latter is meant in the wide sense of sending a text possibly with images.

Child pornography laws have developed over time to cover a wide range of images and texts involving minors. Penalties associated with child pornography offences have also increased significantly over recent decades. In 2004 child pornography laws were altered to include images of people aged 16 and 17 years old, which has created an anomalous situation in which the age of consent does not correlate with child pornography offences. This means that while it is lawful for a 16- or 17-year-old to engage in sexual activity, it is unlawful for an image to be captured of that sexual activity. A range of criminal offences can currently be applied to sexting, depending on the circumstances in which the sexting occurs. For young people, child pornography offences may apply. Commonwealth criminal legislation, both for child pornography and for using a carriage service to menace, harass, or cause offence, may also apply. Sexting may also, depending on the circumstances, breach laws surrounding the use of surveillance devices, and laws relating to coercive offences, such as stalking and blackmail. Therefore sexting among the under age group should be considered as child pornography.

2. ***If you refer back to Figure 8.1 on page 228 where would you place adult sexting- a minor ethical violation, a serious ethical violation, or a very serious ethical violation? What circumstances- consequences, a society's opinion likelihood of effect, time to consequences relatedness, and reach of result- might have adult sexting from a minor ethical violation to a serious ethical violation and then finally on the very serious ethical violation?***

ANSWER

Referring to figure 8.1 which shows the ethical structure I would place adult sexting into serious ethical violations. Consequences, society's opinion likelihood of effect, relatedness, and reach of result may differ between adult and minor.

	Adult	Minor
Consequences	May not be so impactful as both party may understand the impact of the action	Impact will be very severe
Society's opinion	Society may consider it as minor ethical violations	Society may consider it as very serious ethical violations

Likelihood of effect The effect will be not be severe if it is mutual Will be severe even if it is mutual, as they are considered as minority and can be considered as statuary rape

Time to consequences Fast Fast

Relatedness Both party would be highly related Both party would be highly related

Reach of result Both the party Both the party and family members will be effected by the action.

3. ***Consider the whole nation of power being tied to sexting, flirting and cheating. From a psychological point of view why might this be true? Do some research with Tiger Wood's extra marital affairs? Could his cheating be tied to his position of power? Is "power" and the temptations that go with it an excuse for such behaviours?***

ANSWER

It may not be true. It's not the entire nation of power which is being tied to sexting, flirting and cheating as people without power tend to sexting, flirting and cheating, just that it does not get into the limelight.

"On November 24, 2009, according to sources of the Daily Beast Nordegren had a phone conversation with Woods' rumoured mistress Rachel Uchitel before The Enquirer broke the first news of the scandal the next day." It is quoted that Woods had a scandal with Uchitel, in the case of Woods we could say that power would have influenced Woods to behave in such a way. "Power" should not be given as a reason who such misbehave. Human should be capable to control temptations no matter in which position they are in .

4. ***What role can and should employers play in limiting (perhaps eliminating) sexting in the workplace? What about employees to employees' sexting? Regarding the latter, what sort of legal liability does an organization have if an employee sends an unwanted and unwelcome sext to another employee or to a customer?***

ANSWER

Employers should impose stricter penalty on those who commit sexting within the organization. Employees to employees' sexting are not acceptable and should be considered as unethical act. Employee may use the act on sexual harassment to curb the issue of sexting in the organization. Employers covered by the federal or state laws prohibiting sexual harassment are required to take reasonable steps to prevent and promptly correct sexual harassment that occurs on the job. One important factor in determining whether an employer has met the requirement to take "reasonable steps" to prevent and/or stop sexual harassment is whether it has issued and distributed to employees a policy prohibiting sexual harassment and informing employees how to make a complaint. Of course, if an employer has such a policy, but doesn't tell employees about it, doesn't train managers how to follow it, or just fails to enforce it, then the employer may not be taking reasonable care. The same may be true if an employer has lawful policies, and trains employees about them, but then fails to adequately investigate sexual harassment complaints once they are made. It is important to note that before an

employer can be held legally responsible for sexual harassment committed by someone who is not the complaining

5. ***These are purely to answer to yourself. Have you ever participated in sexting? Have you received a sext? Has learning about ethics and non-privacy of technology-enabled communications reshaped your thinking about participating in questionable activities like sexting?***

ANSWER

No, I have never participated in sexting or received any form of sexting. Yes learning about ethics and non-privacy of technology-enabled communications reshaped my thinking about participating in participating in questionable activities like sexting.

SONY REEL FROM MULTIPLE HACKER ATTACKS

1. ***Do some research on the Sony PSN Debacle. What is the new cost estimate for the incident? How many customers has left Sony due to that incident? Have there been any reports of fraudulent use of identities obtained from the hack? Has Sony's PlayStation Network been hacked again?***

ANSWER

Sony has received harsh criticism for failing to quickly publicly acknowledge a security intrusion had taken place. The service was down for six days before Sony admitted that their network security had been compromised and that thieves had swiped personal account information including names, addresses, passwords and possibly even credit card numbers. The PlayStation Network is used by an estimated 77 million subscribers worldwide. The cost of damage is estimated around 17.7 million.

As many as 10 million credit cards may have been exposed, though their information was encrypted, unlike the PSN account personal information. Sony executives at the press conference underscored that the company has not confirmed any cases of credit card fraud associated with the break in, and will let the public know when they have more information.It is stated that around 93,000 accounts (huffington post) had their account hacked.

2. ***Gaming and virtual services in the internet like Sony's PSN, World of Warcraft, and Second Life, boast millions of users. For each of users, the service must store credit card information and personally identifiable information. What must these organizations do to protect the private information of their customers? Is it even reasonable to assume that any organization can have protection measures in place to stop the world's best hackers?***

ANSWER

Organizations should play roles such as listed below;

1. Accountability. Organizations are accountable for the protection of personal information under their control.

2. Identifying purposes. The purposes for the collection of personal information must be identified prior to or during the collection.

3. Consent. Organizations may collect, use and disclose personal information only with the knowledge and consent of the individual (with limited exceptions specified in personal information protection laws).

4. Limited collection. The collection of personal information is limited to what is necessary for the identified purposes and must be collected by fair and lawful means.

5. Limiting use, disclosure and retention. Personal information must be used and disclosed only for the purpose(s) intended, except where consent of the individual is obtained or as required by law. It can be retained only for the period of time required to fulfill the intended purpose(s).

6. Accuracy. Personal information must be complete, accurate and current.

7. Safeguards. An organization in control of personal information must ensure the information is protected by adequate safeguards.

8. Openness. An organization's privacy policies and practices must be readily available to individuals upon request.

9. Individual access. An individual has the right to access his/her personal information, subject to legislated exceptions, and has the right to seek correction.

10. Challenging compliance. Organizations must provide the means for an individual to challenge the organization's compliance with these privacy principles

It is possible for an organization to have world class protections method to safeguard customer information however Hackers never give up in breaking the "code".

3. ***If an extremely intelligent is caught by a law enforcement agency, should that hacker be prosecuted and sent to jail? Is there perhaps a way that the hacker might be "turned" for the good of the digital world? What would that be?***

ANSWER

If a hacker is caught he or she should be prosecuted as it is against the law to conduct such an offence. Yes hackers if "turned" they can be an asset to the country. These hackers can be used to hack the computer system of terrorist countries. For example white hat hackers.

4. ***Every survey taken of businesses regarding data breaches has found that many business are reluctant to publicly announce a data breach. Further, most businesses will downplay the significance of the breach. Why do organizations behave like this? What is there to gain by not operating in a transparent fashion? Is this an ethical issue, a legal issue, or both?***

ANSWER

A data breach is the intentional or unintentional release of secure information to an untrusted environment. Other terms for this phenomenon include unintentional information disclosure, data leak and also data spill. Business tends hide data breaches to retain customers and its good name. Most such incidents publicized in the media involve private information on individuals, i.e. social security numbers, etc. Loss of corporate information such as trade secrets, sensitive corporate information, details of contracts, etc. or of government information is frequently unreported, as there is no compelling reason to do so in the absence of potential damage to private citizens, and the publicity around such an event may be more damaging than the loss of the data itself. This is an legal issue as organization is entitled to allow the customer know about any data breaches that has occurred in the organization so that consumer themselves are able to equipped themselves to protect themselves.

5. ***What's your personal identity theft story? Has someone used your credit card fraudulently? How many phishing email have you received in the last year? How often do you check your credit card report?***

ANSWER

I personally do not have a personal identity theft story. And glad fully I have never been involved in a credit card fraud. Phishing is the act of attempting to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Most of the time emails sent to me will be filtered by the system as I have set in such a manner. I will send those emails to my spam inbox. I do not have a credit card so I do not check my credit card report.