Google Street View cars

In 2006, an engineer developed code that would be used within Google Street View cars. The following roleplay is summarized from this OPC article: `https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2011/pipeda-2011-001/#collection`

1. Google: We did intend to collect WiFi parameters:
    - Publicly broadcast WiFi SSID
    - MAC addresses (unique identifiers for routers)
2. Google: We did *not* intend to collect payloads (messages) sent over open (unencrypted and non-password-protected) WiFi networks
3. OPC: "This is a secret and sweeping collection of data from open WiFi networks across Canada"
4. Google: Oopsie. Let's turn off those Street View Cars (May 2010).
5. Google: Does the data shared over open WiFi networks count as personal information?
6. OPC: This data becomes personal when it can be used to identify someone.
7. OPC: We found full names, phone numbers, addresses, emails, IP addresses, machine hostnames, and the contents of cookies, instant messages and chat sessions. We also found login credentials, details of legal cases, and medical information.
8. Google: But the people used open WiFi networks. Too bad that their personal information got snooped on?
9. OPC: No — the problem is, the collected information is unrelated to the purpose of the Google Street View Cars (mapping out roads).
10. OPC: Google shouldn't even have been collecting it; the fact that it's a bad security practice for people to send private data over open WiFi networks doesn't matter.
11. OPC: Google never intended to collect payload data – or to use it. This implies Google cannot identify the purposes for collection or seek users' consent.
12. OPC: *Even* the information that Google intended to collect (WiFi parameters) is unrelated to the main purpose of Google Street View cars, which is to generate maps.

Questions:

1. What FIP/FIPs is/are violated? Why?
2. What could Google have done differently?
3. Did Google get anything right?

Twitter

Background: Recall that in the "Securing yourself and others" class, we discussed that authenticating people is validating that someone is who they claim they are. We discussed authenticating people through passwords, passports or fingerprints. The following paragraphs are from:
`https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads`

Twitter in 2013 began asking users to provide either a phone number or email address to improve account security. For example, the information was used to help reset user passwords and unlock accounts the company might have blocked due to suspicious activity, as well as for enabling two-factor authentication. Two-factor authentication provides an extra layer of security by sending a code to either a phone number or email address to help users log into Twitter along with a username and password.

From 2014 to 2019, more than 140 million Twitter users provided their phone numbers or email addresses after the company told them this information would help secure their accounts. Twitter, however, failed to mention that it also would be used for targeted advertising, the FTC alleged. Twitter used the phone numbers and email addresses to allow advertisers to target specific ads to specific consumers by matching the information with data they already had or obtained from data brokers, according to the FTC complaint.

1. Twitter: We're collecting users' phone numbers for two-factor authentication.
2. Twitter: We're actually going to use them to show targeted advertisements on the platform
3. FTC: Uh-oh. Users were not informed of this secondary use in the privacy policy.
4. FTC: Users did not meaningfully consent to this use of their phone numbers.
5. FTC: Goes ahead and fines Twitter for *deceptively* using phone numbers for the secondary use of advertising.

Questions:

1. What FIP/FIPs is/are violated? Why?
2. What could Twitter have done differently?
3. Going forward, what did the FTC require Twitter to do? (You can use the link to FTC's article above.)

BetterHelp

The paragraph below is paraphrased from:
`https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook`

Background: Consumers interested in BetterHelp's services must fill out a questionnaire that asks for sensitive mental health information—such as whether they have experienced depression and are on any medications. They also provide their name, email address, birth date and other personal information. This information is used to match patients to therapists. At several points in the signup process, BetterHelp promised consumers that it would not use or disclose their personal health data except provide counseling services. Despite these promises, BetterHelp shared consumers' email addresses, IP addresses, and health questionnaire information to Facebook, Snapchat, Criteo, and Pinterest, for advertising purposes. BetterHelp was fined by the FTC: "BetterHelp will be required to pay 7.8 million USD for deceiving consumers after promising to keep sensitive personal data private."

Questions:

1. What FIP/FIPs is/are violated? Why?
2. What could BetterHelp have done differently?
3. Going forward, what did the FTC require BetterHelp to do? (You can use the link to FTC's article above.)

Mariott

Background: Mariott had their databases breached in 2018. Out of all database records that were breached, the oldest ones were made in 2002. The OPC investigated this data breach. The information below is summarized from:
`https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2022/pipeda-2022-005/`

1. Mariott: Our policy is to retain data for 10 years due to the Alberta Corporate Tax Act
2. OPC: Okay (squints hard), but what about other data items that are not relevant for tax purposes?
3. OPC: Mariott, you did not need to keep other Canadians' data for 10 years.
4. OPC: Mariott, you did not need to keep Albertans' non-financial data (e.g. passport numbers, guest reservation details) for 10 years.
5. OPC: Mariott, you should've deleted these data items by 2012 — they would not have been breached!

Questions:

1. What FIP/FIPs is/are violated? Why?
2. What could Mariott have done differently?
3. Going forward, what did the OPC require Mariott to do? (You can use the link to OPC's article above.)

Apple

Background: To download free apps, Apple required users to create an Apple ID. Creating the Apple ID required the user's date of birth and their payment information (credit card details). The OPC investigated a compliant about this. The following information is taken from:
`https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201314/2013_pipeda/#heading-0-0-0-4-1`

In a case tied tightly to online privacy transparency, an individual alleged that Apple Canada should not have required him to supply certain data during the process of creating his Apple-specific identifier, known as an Apple ID, which was needed to download a free application from the Apple website. The process called for payment information, such as a credit card number and a date of birth.

Upon investigation we concluded that Apple had a legitimate right to use birthdates to help authenticate the identities of several million Canadian customers. However, we noted that the company's privacy policy did not fully explain this practice. Apple agreed to update its policy. In anticipation of this clarification, we deemed this aspect of the complaint to be well-founded and conditionally resolved.

With respect to the collection of financial information, Apple stated that its website's support section contained instructions for downloading free apps without providing payment information. According to Apple, using the search term "credit card", one of the search results would enable users to learn that the payment card requirement could be bypassed by following a specific alternative process.

We reviewed hundreds of comments from frustrated users in an Apple open forum, and conducted our own technical analysis. We concluded that the workaround for the free apps was not evident, and that Apple did not make its policies and practices on the collection of credit card data clear to users at the relevant time—namely when a user registered for an ID.

We were concerned that Apple's practices could result in the over-collection of sensitive payment information.

We deemed this aspect of the complaint to be well founded, and recommended that Apple clearly communicate to users that a form of payment is not required when registering for an Apple ID for the purpose of downloading a free application. We recommended that Apple could achieve this by adding the option of proceeding without the need to supply payment information at every point of registration. In response to our final report of findings, Apple agreed to our recommendation.

Roleplay:

1. Apple: We need the date of birth and their payment information to authenticate users.
2. Online forums: Uhh no that's not okay. OPC you seeing this?
3. OPC: Ok. Apple, taking the date of birth as input while creating an Apple ID is OK.
4. OPC: But your privacy policy doesn't say that the date-of-birth is needed to authenticate users. Update it.

5. OPC: Apple, taking the payment information, while the user is trying to download a free app, is not OK.
6. Apple: *Well actually,* users can create an Apple ID without providing payment info.
7. Apple: All they need to do is search "credit cards" on our webpage and they would've known.
8. OPC: Nope. Apple, you don't need the payment info to download a free app. You're overcollecting. (Principle 3)
9. OPC: Also, Apple, seeing those confused & dissatisfied consumers on those online forums above?
10. OPC: You'd better provide a button or something right where the user is creating the Apple ID, so that they know they don't need to supply payment info.

Questions:

1. What FIP/FIPs is/are violated? Why?
2. What could Apple have done differently?
3. Going forward, what did the OPC require Apple to do? (You can use the link to OPC's article above.)

Privacy breach risk self-assessment

Recall the Canada Computers case that we discussed in class. Consumers who bought items from Canada Computers were concerned about their data being exposed in the breach. Consumers claimed that Canada Computers should have informed the Office of the Privacy Commissioner (OPC) of the breach.

An organization is only legally required to report breaches to the OPC if there is a "real risk of significant harm (RROSH)". The risk of significant harm depends on the sensitivity of the information breached and the likelihood of its misuse. The OPC has released a privacy breach risk self-assessment guide here: `https://services.priv.gc.ca/rrpg-rrosh`. This tool takes as input the sensitivity of the information breached, the incident response steps taken to handle the breach, and estimates the likelihood of its misuse. It outputs the potential risks that the breach presents to an impacted individual.

Consider the following resources for this task:

RA Breach report made by a consumer on Reddit, as we discussed in class: `https://www.reddit.com/r/bapccanada/comments/1qk4axy/canada_computers_online_card_skimmer/`. The post includes what sensitive information was exposed in the breach, and estimates of when the breach may have occurred.

RB The following comment on this post discusses who received the breach information: `https://www.reddit.com/r/bapccanada/comments/1qk4axy/comment/o13v3xu/`. You may use `https://lookup.icann.org/en/lookup` to verify the claims in this comment.

RC Canada Computer's email response is available here: `https://www.reddit.com/r/bapcsalescanada/comments/1qn80rr/comment/o1rte9z/`.

Questions:

1. Fill out the privacy breach risk self-assessment for the Canada Computers breach. To fill out the questionnaire, consider the resources mentioned above. You may need to estimate responses to one question.

2. Describe how you arrived at the response for the following questions (questions 3, 5, 7 & 12) in the questionnaire. Mention which resources (resource A, B or C) you used to answer each question. If you did not receive a particular question when filling out the questionnaire, answer this question anyway, based on these resources.

   Q3 What types of personal information were breached?

   Q5 What type of breach is it? Which best describes how the personal information was breached?

   Q7 Who received or obtained the breached personal information? Which best describes the recipient(s) of the personal information that was received either in error or through malicious means?

   Q12 How much time elapsed between the beginning of the breach and the time at which it was contained?

3. What are the potential risks to the consumers of Canada Computers whose data was breached?

4. Should Canada Computers have reported the breach?