Big Data and Privacy Course:

Evaluation (legal and knowledge-processing aspects of privacy)

Preamble

These basic guidelines are intended to guide you through the identification of some of the potential impacts the App you are assessing might have on individuals' privacy. The broader societal impact of the App (ethical and proportionality aspects) is not included in the assessment. We however ask you to briefly reflect upon these aspects by analyzing the viewpoint of a stakeholder external to the App.

We start from the premise that the App is used in full compliance with the legal framework. This means that you should work with the assumption that the App is collecting users' data with their consent, and that this includes, for example, the users who took an Instagram photo, checked into a venue, etc. You do not have to assess this aspect.

This assignment focuses on four **stakeholders**:

1) Individuals from/about whom the data are collected
2) Users of the App (third parties that use the App to obtain analysed/aggregated information)
3) App designer
4) External party (who does not use the App but is affected by it indirectly)

For 2) and 4), we will propose a specific App user type respectively external party type, depending on the descriptions of the data analysis and the App. This will follow in a separate mail to your student working group.

For the assignment, please designate 1 person each from your 4(5)-person student group to take the perspective of that stakeholder. We propose you proceed as follows in order to make sure all stakeholders' views are represented:

1. Collectively: Assign the stakeholder roles.
2. Individually: (re-)read the analysis and App description and begin to "think from this role".
3. Collectively: Work on question 1 (data flows). It is crucial that there is one answer to this that your whole group agrees on.
4. Individually: answer questions 2 and 3. It is to be expected that these answers differ according to which stakeholder role you assume.
5. Collectively: work out answers to question 4. In this phase, different opinions between the stakeholders may occur – this is a feature not a bug, but in the end you will have to come up with a joint proposal. In that joint proposal, you may, but do not have to, describe differences you encountered and how you resolved them.

Please work this out in writing and present it orally. We expect ~ 5 pages per group for the final written version, and plan for 30 minutes including discussion per group.

1. Please send a first version to "your KaW project group" (will be identified in a personalized email), and Cc Bettina Berendt and Fanny Coudert (bettina.berendt@cs.kuleuven.be, fanny.coudert@law.kuleuven.be), by Dec. 8th so that the others have a chance to think about it.
2. Please present your results in the exercise session on Dec. 10th. Your KaW project group will comment. The assignment of groups to the morning or afternoon session will follow.
3. You may want to revise your written version. Please send the final version to us (bettina.berendt@cs.kuleuven.be, fanny.coudert@law.kuleuven.be) by Dec. 19th.

Guidelines for initial privacy impacts assessment and related design advice

Fanny Coudert and Bettina Berendt

November 2014

http://people.cs.kuleuven.be/~bettina.berendt/teaching/kaw/guidelines.pdf

1) **Describe information flows: Explain how information will be obtained, used, retained and shared**

   This should include a description of (a) how data are collected, (b) who has access to which data for which purposes, (c) how data are processed, (d) how new knowledge is generated and shared with users.

   You can do this informally (e.g. with simple flowcharts) or use an appropriate modelling language, for example UML collaboration or interaction diagrams

2) **Identify the drivers each party has in disclosing, collecting, using, sharing the information:**

   • Individuals: reasons for disclosing information and expectations with regard to the use of this information

   • Data handlers: reasons for collecting, using, sharing the information (purpose of the data processing activity)

3) <u>Identify how the app will impact individuals' privacy (describe briefly what kind of problem can arise). You can give a "story", e.g. a possible misuse case.</u>

In order to assess the impact the App might have on individuals' privacy, you should take into account two elements: (1) the privacy expectation of the individual whose data is being processed and (2) the purpose for which the data is being processed (goals of your application).

For the first element (1), please consider that these individuals may be:
a) users of the platform (one type of ppl whose data may be processed by the app)
b) users of the app (another type of ppl whose data may be processed by the app)
c) others?

For the second element (2), please consider that each stakeholder might have different purposes:
a) App developer: main goal of the App. Note that one App might pursue different purposes
b) Third parties accessing the aggregated information (or the new knowledge generated by the App): they pursue their own goals
c) others?

There may be stakeholders whose privacy is not affected (e.g. the app designers, stakeholder 3", are typically not affected). However, you may find that your assumed point of view affects the results: For example, if you assume the role of the app designer, you may have a very different perception of how your app affects its users than if you are one of these users themselves. If this happens during your work on this question, annotate your description roughly like this: "From stakeholder 3's point of view, stakeholder 2's privacy may be impacted as follows: ... From stakeholder 2's perspective, the following potential problem should be added: ..."

See slides of lecture of 8/10 for definition and examples

- ☐ Privacy of the person (body privacy)
- ☐ Privacy of behavior and action
- ☐ Privacy of communication
- ☐ Privacy of data and image
- ☐ Privacy of though and feelings
- ☐ Privacy of location and space
- ☐ Privacy of association

4) **How would you advise designers to limit the impact on individuals' privacy?**

Concretely, how would you advise system designers to integrate the following considerations into the design of their system? (Please select the most relevant for your use case.)

- **Data minimization**:
  - how do you limit data collection to what is strictly necessary for the purpose of the processing?
  - Do you anonymize the data and how?
- **Use limitation (further uses):**
  - In relation to the **inferences** drawn from the data (generation of new knowledge), to what extent this use of the data aligns with the consent initially given by individuals (reasonable expectations of individuals)?
    - In case it does not align, you either have to:
      - Come back to individuals to obtain their consent for this new data processing activity
      - Justify that the data processing activity can be based on legitimate interests of the app developer. This means that you should justify that this interest outweighs individuals' rights. Concretely, you should be able to argue *that (a) the App is reasonably likely to achieve its objectives, (b) the App is necessary to achieve the purpose of the processing and there is no other less (privacy)intrusive means that would allow to reach the same objective, (c) the App is designed in such a way as to minimize the impact on individuals' privacy*).
    - What additional measure do you take to protect individuals' privacy in this specific context? Briefly describe the measure, and how this measure would address the concerns raised.
  - Have you defined a **data retention period**?
- **User empowerment:**
  - Information rights:
    - How do you inform individuals at the moment of collection and of further uses?
    - Which information do you provide?
  - Have you considered to implement consent in a dynamic way, e.g. to allow individuals to give their consent in a granular way (only to certain data processing activities and for a limited period of time).
  - How do you involve individuals in the data processing activities:
    - Do you enable individuals to access the information that is processed about them?
    - Have you implemented mechanisms to enable individual to access/rectify/request deletion of their data?
- **Accountability**:
  - How do you ensure the App designer is processing the data in the way individuals were informed it would be? Are any safeguards implemented to trace data uses for further audits?
  - How are data retention periods enforced?

Acknowledgements

We have developed these guidelines based on privacy impact assessments used in practice as well as our own work.

- See for examples of PIA e.g. ICO: http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/pia-code-of-practice-final-draft.pdf
- See other examples:
- Overview: http://www.piafproject.eu/ref/PIAF_D1_21_Sept_2011.pdf
- US: https://www.sec.gov/about/privacy/piaguide.pdf
- New Zealand: https://www.privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment-handbook/
- Canada: https://www.priv.gc.ca/resource/fs-fi/02_05_d_33_e.asp
- Australia: http://www.oaic.gov.au/privacy/privacy-archive/privacy-resources-archive/privacy-impact-assessment-guide

Here is our (high-level) reasoning about the multi-stakeholder approach:

- Morton, Anthony; Berendt, Bettina; Gürses, Seda; Pierson, Jo. "Tool Clinics" : Embracing multiple perspectives in privacy research and privacy-sensitive design, Dagstuhl Reports, volume 3, issue 7, pages 96-104, 2013 (PDF)

In the future, we also plan to investigate / integrate elements from further methods, for example LIND(D)UN, developed at KU Leuven.

Bettina Berendt and Fanny Coudert, November 2014.