Data privacy: an introduction (part 1)

Klara Stokes

What is privacy?

Privacy has been defined in many ways over the years.

Usually privacy is concerned with the individual human being.

We may talk about privacy as the **control over your own personal information**.

Personal information: examples from modern life

Shopping

- I have a fidelity card (*kundkort*) at the supermarket where I buy my food. Am I comfortable with the supermarket analyzing my food habits? Can they tell when/if I have PMS? Or if get pregnant?

Personal information: examples from modern life

Shopping

- I have a fidelity card (*kundkort*) at the supermarket where I buy my food. Am I comfortable with the supermarket analyzing my food habits? Can they tell when/if I have PMS? Or if get pregnant?
- My pharmacy belongs to a corporate group which also owns my insurance company. Can they use knowledge about my diseases they got from the medicine I buy to increase what I pay in insurance premium?

Personal information: examples from modern life

Digital and mobile communications

- When I write a personal email to my father we discuss incontinence. Suddenly I start getting advertisments on adult diapers for men in my browser. Is this ok?

Personal information: examples from modern life

Digital and mobile communications

- When I write a personal email to my father we discuss incontinence. Suddenly I start getting advertisments on adult diapers for men in my browser. Is this ok?
- My mobile network operator can register the position of my mobile phone with high precision (also without GPS). I am where my phone is. They collect my position 24 hours/day. When they share this information for research purposes (e.g. infrastructure planning), can people tell where I have been?

Personal information: examples from modern life

Digital and mobile communications

- When I write a personal email to my father we discuss incontinence. Suddenly I start getting advertisments on adult diapers for men in my browser. Is this ok?
- My mobile network operator can register the position of my mobile phone with high precision (also without GPS). I am where my phone is. They collect my position 24 hours/day. When they share this information for research purposes (e.g. infrastructure planning), can people tell where I have been?
- When on the internet I always use the same search engine. When I suspect that I have got a disease, I search for that disease. Probably the search engine knows more about my medical history, than my doctor does.

Personal information: examples from modern life

Medicin

- I am interested in family history so I send a sample of my DNA (some spit in a cup) to a company in genealogy research. What if someone later uses this sample to get information regarding possible genetic diseases I have? What if the company is bought up by some other company?

Personal information: examples from modern life

Medicin

- I am interested in family history so I send a sample of my DNA (some spit in a cup) to a company in genealogy research. What if someone later uses this sample to get information regarding possible genetic diseases I have? What if the company is bought up by some other company?
- From the 1960's, all newborn babies in Sweden take a PKU test (a blood sample). This test is saved and can be used for research later. Is it justified to include people in research investigations without asking? (Babies can't claim their rights.) What if policies are changed and the test could be used for other purposes?

Personal information: examples from modern life

Cars

- In my smartphone I have an app telling me where my car is at every moment. Who else can access this information? What about the people at the service station? What about thieves? Can they tell when I am not at home?

Personal information: examples from modern life

Cars

- In my smartphone I have an app telling me where my car is at every moment. Who else can access this information? What about the people at the service station? What about thieves? Can they tell when I am not at home?
- My friend has a more modern car than I do. Her car talks to the other cars about obstacles in the road, ice, etc. How much can the other drivers find out about her from the information sent by the car?

Personal information: examples from modern life

At work

- At my workplace they started a new ergonomic program. Sensors will tell when I sit or stand in a way which could be harmful. They say they erase data after it is used. Is this enough to protect my privacy? Will they also be able to tell how often I go to the toilet?

Personal information: examples from modern life

At work

- At my workplace they started a new ergonomic program. Sensors will tell when I sit or stand in a way which could be harmful. They say they erase data after it is used. Is this enough to protect my privacy? Will they also be able to tell how often I go to the toilet?
- The production at my workplace is monitored in order to increase efficiency and to optimize the work-flow. Will they also be interested in decreasing my salary since I'm so slow?

Personal information: examples from modern life

At work

- At my workplace they started a new ergonomic program. Sensors will tell when I sit or stand in a way which could be harmful. They say they erase data after it is used. Is this enough to protect my privacy? Will they also be able to tell how often I go to the toilet?
- The production at my workplace is monitored in order to increase efficiency and to optimize the work-flow. Will they also be interested in decreasing my salary since I'm so slow?
- The taxi I drive has a GPS, sending my position to the call center. When I drop off Adam, 7 years and autistic, it is my responsibility to check that he arrives safe inside. But he falls, hits his head and then starts crying. A big mess. I feel stressed by the GPS so I just tell him to get inside and then I drive off.

Personal information: examples from modern life

Industry

- At my company we use a cloud service to store all the data about clients. The servers of this cloud are located in the US. Under the laws of what country does these data fall? Is it legal to keep personal data about individuals at servers outside Sweden?

Personal information: examples from modern life

Industry

- At my company we use a cloud service to store all the data about clients. The servers of this cloud are located in the US. Under the laws of what country does these data fall? Is it legal to keep personal data about individuals at servers outside Sweden?
- Two companies want to share information about their customers. How can they do this without violating the privacy of the customers, nor revealing secrets about their own organization?

Privacy

Privacy is **control over your own personal information**. Do you have control?

Privacy

Privacy is **control over your own personal information**. Do you have control?

But so what! I live in Sweden, certainly the authorities will make sure they have control, right? Anyway, who cares, I don't have anything to hide.

Privacy

Privacy is **control over your own personal information**. Do you have control?

But so what! I live in Sweden, certainly the authorities will make sure they have control, right? Anyway, who cares, I don't have anything to hide.

But privacy is not about having something to hide. It is about how **normal decency** can be kept also **after digitalization**.

Control?

So who is in control?

The entities who develop the products and services should be aware of possible privacy issues they could cause. They should **design with privacy in mind**.

Authorities write laws to control the use and misuse of information about individuals.

Stakeholders should be aware of and understand the new laws. Do you understand?

(In May 2018 the new European General Data Protection Regulation comes in action. Do you think this affects your research?)

Data privacy

Data privacy is about controlling personal information in data.

Control can take place by the individual before data is collected (user privacy), or after collection, but before data is shared or used by third parties (sanitization).

Main methods:

- Encryption: make information secret / useless to outsiders - only someone with the correct key can read it.
- Data masking: keep information useful to outsiders - drop only what can be linked to individuals.