About the hypertext version

When reading the hypertext version, people can click links to read different parts of the thesis. Each part will consist of about 5 to 10 sentences with a title and explains one aspect of my graduation. Every part will have at least two links that refer to the next and previous part of the thesis (except first and last part). By clicking these links a reader can go back and forth in the thesis and read it from A to Z and back again. However a reader is also capable to skip parts it already knows, refer back to parts it forgot and jump to sections which are of high value to the reader. The readers can identify the content of different parts by reading what the links to those parts say. I'm thinking about anonymously tracking which parts are read. I also want to enable readers to inform me about which parts they don't understand, by clicking a button at parts they didn't grasp.

A hypertext is usually written in HTML. However I want to be able to write in a classic text editor and not be bothered by technical details when writing. Therefore I'll first write the thesis in a pseudo hypertext format. Links will start with <<< followed by the text will be readable in the link. Then comes the = sign followed by a reference to which part the link will link. A link is ended with >>>. Here's an example of a sentence with a <<<link = this paragraph>>>. In this example a link that reads “link” refers to the paragraph it's appearing in. When a link points to a specific part I'll use “ to enclose the title of that part.

By reading a hypertext version of my thesis, people have a lot more freedom to choose what they read. Instead of having to go through 8000 words they select parts by clicking on links that interests and concerns them. Tracking the readers may help me to understand how readers in general are reading my thesis. Similarly any reports on which parts are not clear will indicate which parts can improve.

Abstract
This thesis explores how people are being <<<tracked online = “You're being tracked”>>>, why this <<<may be a problem = ways to exploit personal data>>> and <<<why the user is not benefited by tracking in anyway = myths about tracking>>>. I also discuss how to <<<prevent tracking from happening = preventive measures>>> and <<<what possibilities companies have = alternatives to tracking>>> to make money without tracking consumers. My <<<project attached to this thesis = “what”>>> is an attempt to make clear <<<which risks and changes are involved = why>>> concerning the huge amount of data that gets generated around our personas <<<in a playful manner = how>>>.

What
My project at first glance looks like a regular Monopoly game. However the streets don't represent streets in Atlantis City or any other city in the world. Instead they portray internet platforms like Facebook, Hotmail, Youtube and Twitter. Therefor it is impossible to buy streets in this game, but it is possible to buy shares, bonds of derivates from these web services. Similarly you can't buy houses or hotels, but you're able to buy data storage and data centers. When players draw a “change” or “community chest” card they tell stories about how social media are leaking data about their users and how people are affected by this.

How
For now I limit my description of how to: a table that states how each element in the original Monopoly game will get restyled to fit the new game reality I want to create.

Monopoly	**WWWonopoly**
Change cards	Messages about data leaks
Public fond cards	Messages about data leaks
Buying/landing on/trading a street	Buying/landing on/trading shares of a platform
Completing streets of a color	Owning a platform
Buying houses	Buy data storage
Buying hotels	Buy data center
Buying/landing on a railway station	Buying/landing on an internet provider
Landing on electricity and water company	Landing on Craigslist and Wikipedia
Get salary	Get salary
Go to prison	Go to prison
Pay taxes	Only two things are sure in life: death and ... ;)
Free parking	Free peer-to-peer downloads
Take a mortgage on property	Possibly: selling the securities with an option to re-buy

A few rules that are nice to add here:

- There is no such thing as the free p2p download jackpot (as the game would last forever)
- Each player begins with two randomly assigned properties for which they must pay (to speed up play)
- A game will last X number of turns

Why
It lies in our nature that we can't assess risks very well. A lot of people like social media, but very few seem to be aware what the risks of them are. By allowing players to take the perspective of somebody with power over the functioning of the social media system, the players get a bird view of what is happening. From this perspective the players are more likely to become aware of risks than when they have a frog like perspective on social media by interacting with the platforms. By playing the game and reading the bits of text and articles that are attached to each game message, the player gets a better sense of how social media function and in which way the player is vulnerable on line. Informing users

in this somewhat playful manner lie could prevent harm.

You're being tracked
When you are online it gets tracked, among other things, which sites you visit and which things you buy. It happens to all of us if you don't <<<take precaution = go to list about what to do>>>. This information is saved for about six months (in some cases longer) and gets used to make money by different parties. This thesis will discuss in which ways information about your behavior online is valuable and how falls into the hands of who is interested in it.

A tracking example
The fact that you are being tracked is problematic when sensitive information is disclosed to parties who were not supposed to have that information. This could happen when you do your groceries online. Insurance companies may keep track of what you eat and adjust your fee, because your eat habits indicate a heightened change for diabetes.

- <<<go to Washington Post to read more on this example = external link to WP>>>
- <<<learn about more examples = invitation to visit the project>>>
- <<<I have nothing to hide = go to next>>>
- <<<Tell me more about tracking = skip pages with arguments to worry about the topic>>>

Nothing to hide
You may think that you don't have anything to hide even when you've read about some <<<examples = "A tracking example">>>. Are your friends and family in the same position? Will you have something to hide as you get older and your medical data becomes more valuable to insurance companies? Aren't there any ways imaginable in which information about you can be used against your interest, although it doesn't happen right now? Surely one of the answers to these questions is yes. In that case it's better to live in a society where you don't have to worry about whether sensitive information gets revealed or not.

- <<<stop reading = go to Google>>>

Remembering the advise
I have made a <<<list of incentives = visit the list>>> which you could follow to better protect yourself from unwanted information disclosure. However a rule, without an explanation of why that rule is important, is just another rule. Such rules are likely to get broken! That's why I want to explain you in simple terms why these rules are important and how they affect your privacy. It will take a little more effort to understand this than to read the bullet point list of incentives. Then again once you understand the incentives you can better protect not only yourself but also others who are in need for it and haven't red this thesis themselves.
Do you know what a browser and a server are?

- <<<I have no idea! = continue normally>>>
- <<<I know what a browser is = skip next page>>>
- <<<I know what both things are = skip next two pages>>>

The browser
When you visit a webpage on a website you're using a computer program that is called a browser. Examples of browsers are Internet Explorer, Firefox, Chrome, Safari and Opera. From these browsers Firefox and Opera are the most independent browsers and considered best at protecting your privacy online.

- <<<read what else you can do to protect your privacy = list of incentives>>>
- <<<continue with thesis = go to next page>>>

A website
A website is a collection of webpages. For now lets think about webpages as being files, which they used to be in the early days of the internet. All webpage files of a website reside on a computer, which is part of the internet infrastructure. As soon as you click on a link to visit a webpage your browser makes connection with a computer which stands in a room like you see below:

Many powerful computers are stored in those things that look like fancy refrigerators on the image. Together these computers are a part of the internet. When you see a webpage in your browser it has been send to your browser by one of these computers, which are called servers. Think about these computers as the devices that **serve** you the internet pages your browser requested for when you click links.

Webpages come in parts!
Your browser receives an entire webpage in parts. The first part, which usually contains all text on the webpage, will also indicate to a browser where it can find other parts. These additional parts may be images, video or audio, that are on the webpage you're visiting. Since these parts are often essential to the look of the webpage your browser will download these parts without checking if they are necessary.

The additional media parts could be located on the same computer as the webpage your visiting, but they could also be coming from completely different computers. A website logo on a webpage is often retrieved from the same computer as that webpage. However some images on webpages are almost never on the same computer as the webpage, that holds those images. Think for instance about Facebooks “like it” buttons or Youtubes video players, but also banners and commercials. These media are retrieved from Facebook, Google or another media company. When that happens the computers, from these companies, not only provide the requested media. They also record that you have received the media when visiting a particular webpage from a particular website!