Appendices

Contents

Appendix 1 Questionnaire & answers

Research on privacy sensitivity about Wifi-access data

Here are a few questions about data privacy sensitivity when you are connected to the campus Wifi. It only takes you 2 to 3 minutes to answer. Thank you for your cooperation!

*Required

1. **Your information will be later used for research purposes. Do you agree to share your information or not? (Choosing 'No' won't affect answering following questions)** *

   Mark only one oval.

   ○ Yes, I agree.

   ○ No, I don't agree.

1/4

2. **Are you a user of the campus Wifi eduroam?** *

   Mark only one oval.

   ○ Yes.

   ○ No. *After the last question in this section, stop filling in this form.*

3. **What is your oppupation in TU Delft?** *

   Mark only one oval.

   ○ I am a student.

   ○ I am an employee.

   ○ I am a visitor.

   ○ Other: ____________________

4. **Are you aware that your personal data is being collected when connecting to the campus Wifi?** *

   Mark only one oval.

   ○ Yes.

   ○ No.

Just a reminder before the following questions: all your answers are anoymous, and will only be used for internal research.

2/4

5. **What kind of data do you think is being collected through campus Wifi? (multiple selection)** *

Tick all that apply.

□ Real time location (your routine)

□ Location at a certain time

□ The time of using the device (when?)

□ Duration of using the device (how long?)

□ What kind of device (e.g. mobile phone/laptop?)

□ What kind of website you visited

□ Downloading behavior

□ Other:

6. **For what kind of purpose do you think the Wifi provider is collecting your data? (multiple selection)** *

Tick all that apply.

□ To improve Internet service.

□ To improve all kinds of campus services.

□ For security reasons.

□ To use the data for research purposes.

□ To sell the data for business purposes.

□ To monitor the Wifi users.

□ Other:

3/4

7. **From 1 to 5, please rate how do you feel about the fact that your personal data is being collected through campus Wifi.** *

Mark only one oval.

	1	2	3	4	5	6	7	
It's totally ok to me. I feel secure.	○	○	○	○	○	○	○	I don't feel secure at all. I feel my privacy is being threatened.

8. **Is there anything you wouldn't like to do when connecting to the campus Wifi? Why?** *

4/4

9. **After you have answered all the questions above, do you agree to share your answers for research purposes? All the answers will be anonymous.** *

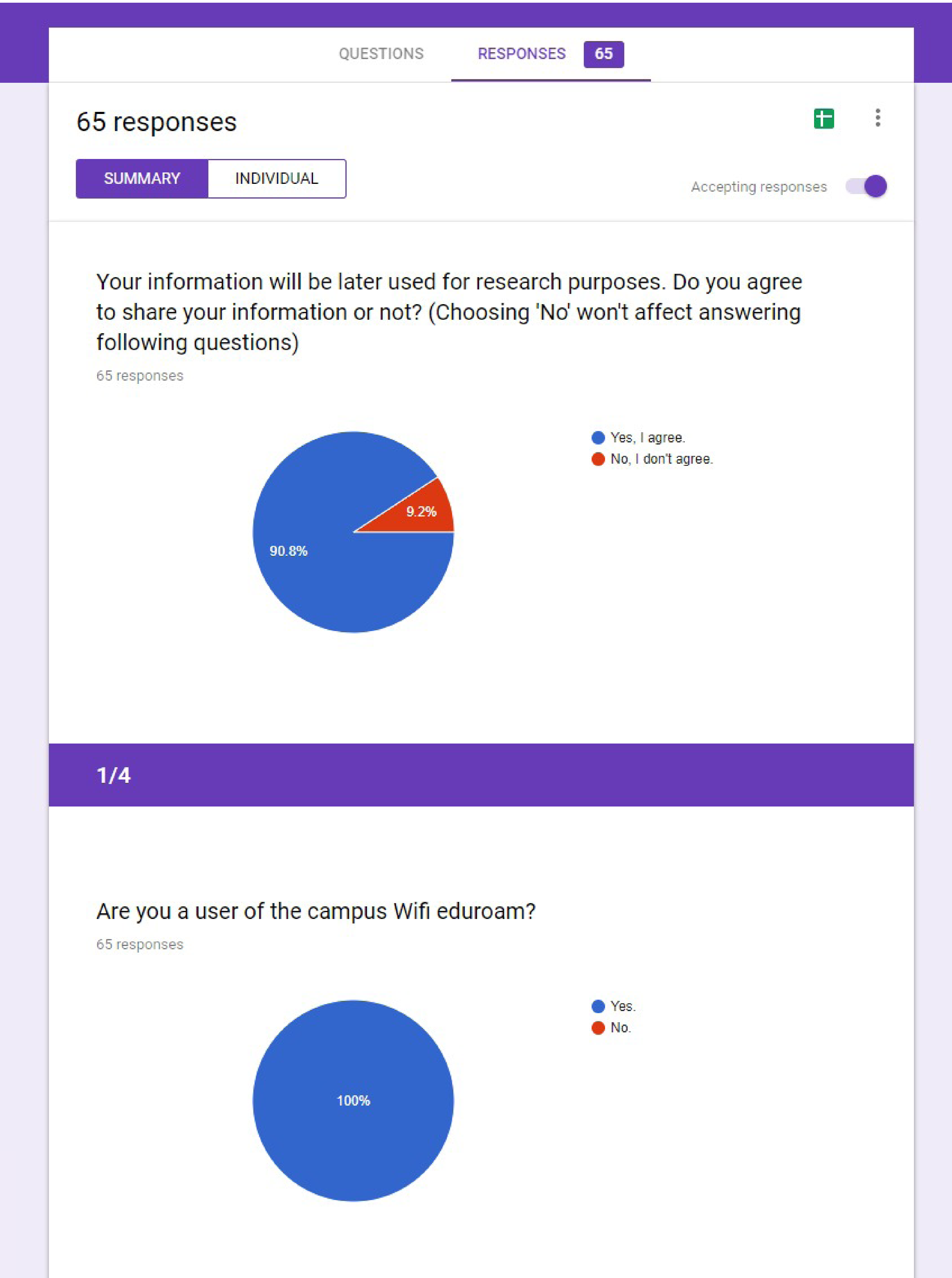
Mark only one oval.

- ○ I chose 'I agree' at the beginning. Now I still agree.
- ○ I chose 'I agree' at the beginning. Now I don't agree.
- ○ I chose 'I don't agree' at the beginning. Now I agree.
- ○ I chose 'I don't agree' at the beginning. Now I still don't agree.
- ○ I don't remember what I chose at the beginning. Now I agree.
- ○ I don't remember what I chose at the beginning. Now I don't agree.

You have completed all the questions.

Thank you again for your answers!

Powered by
Google Forms



65 responses

Your information will be later used for research purposes. Do you agree to share your information or not? (Choosing 'No' won't affect answering following questions)

65 responses

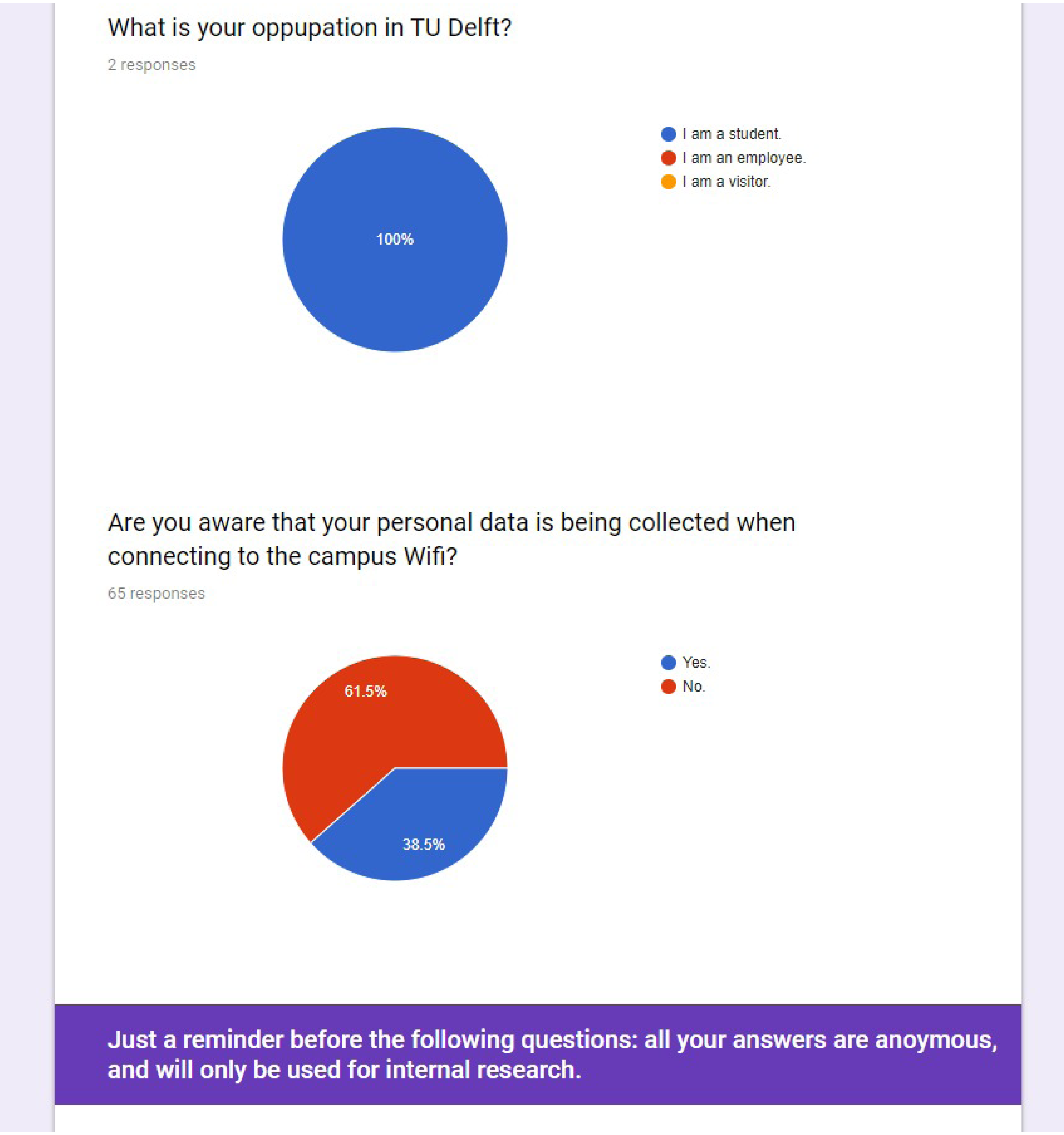
● Yes, I agree.
● No, I don't agree.

1/4

Are you a user of the campus Wifi eduroam?

65 responses

● Yes.
● No.



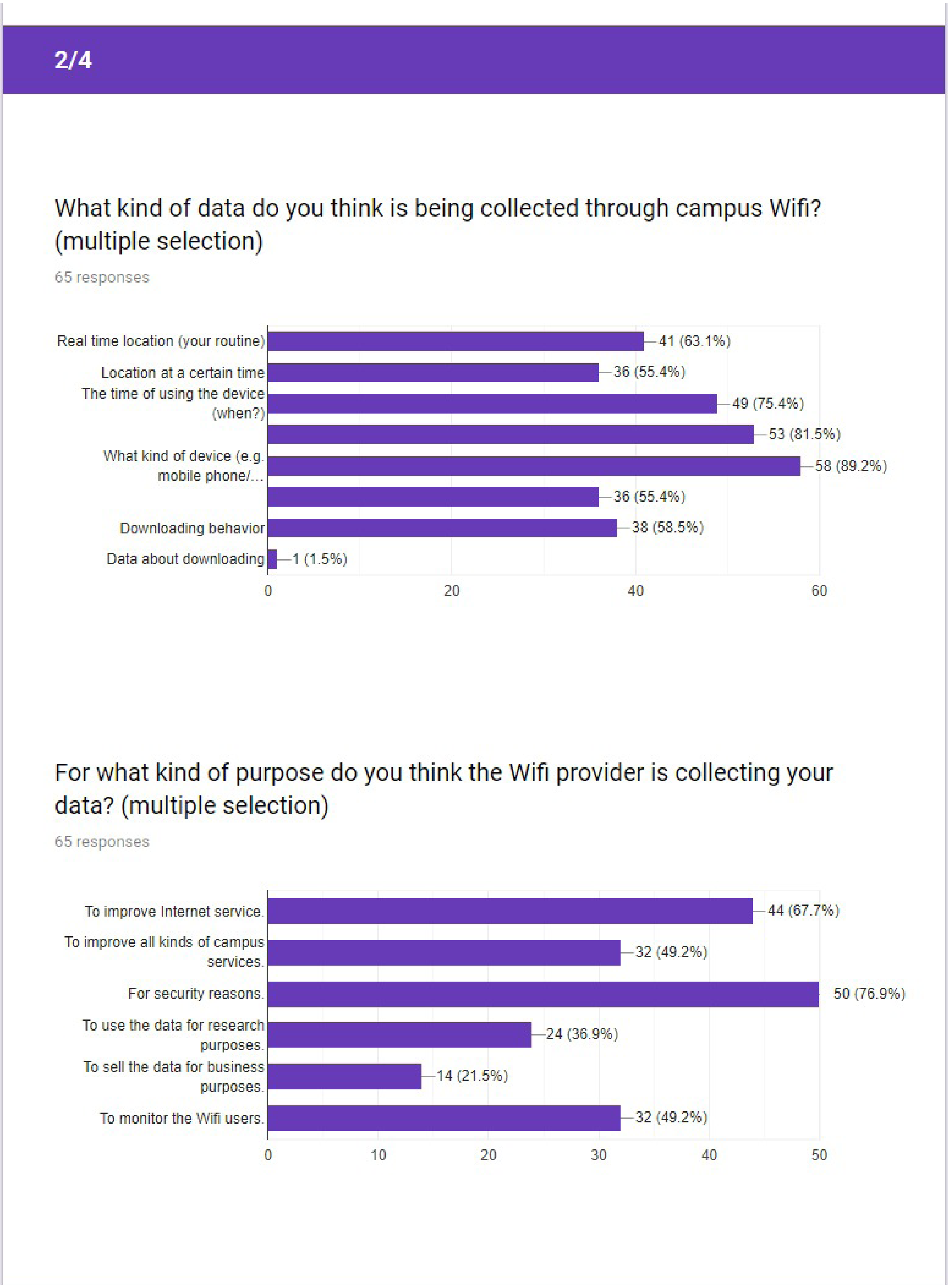
What is your oppupation in TU Delft?

2 responses

Are you aware that your personal data is being collected when connecting to the campus Wifi?

65 responses

Just a reminder before the following questions: all your answers are anoymous, and will only be used for internal research.



2/4

What kind of data do you think is being collected through campus Wifi? (multiple selection)

65 responses

Real time location (your routine)
41 (63.1%)
Location at a certain time
36 (55.4%)
The time of using the device (when?)
49 (75.4%)
53 (81.5%)
What kind of device (e.g. mobile phone/...
58 (89.2%)
36 (55.4%)
Downloading behavior
38 (58.5%)
Data about downloading
1 (1.5%)
0
20
40
60

For what kind of purpose do you think the Wifi provider is collecting your data? (multiple selection)

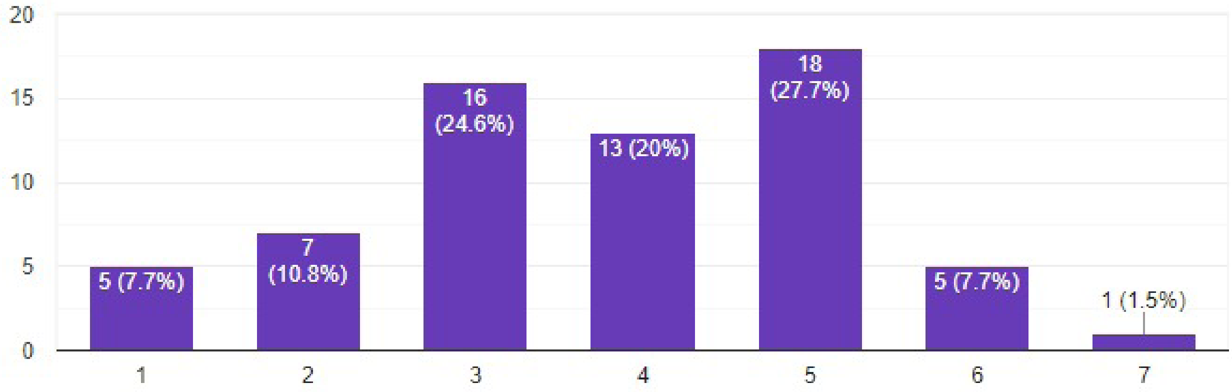
65 responses

To improve Internet service.
44 (67.7%)
To improve all kinds of campus services.
32 (49.2%)
For security reasons.
50 (76.9%)
To use the data for research purposes.
24 (36.9%)
To sell the data for business purposes.
14 (21.5%)
To monitor the Wifi users.
32 (49.2%)
0
10
20
30
40
50

3/4

From 1 to 5, please rate how do you feel about the fact that your personal data is being collected through campus Wifi.

65 responses



Is there anything you wouldn't like to do when connecting to the campus Wifi? Why?

65 responses

No

no

nothing

Not really.

No, Never thought about that

watch the porn (LOL)

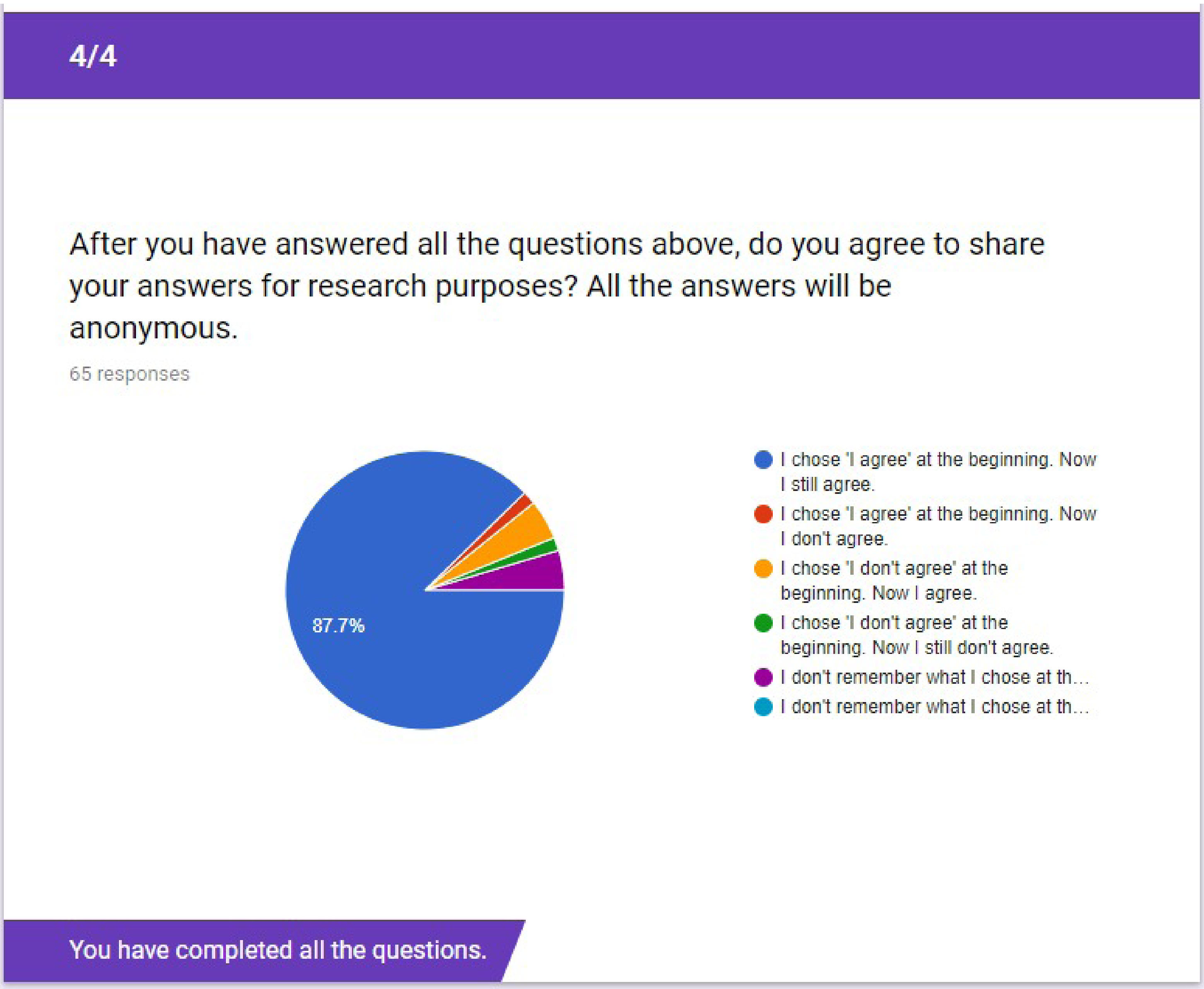
Nothing

I feel quite okay doing anything that I normally do

Nothing specific. But now I will be a little bit concerned about my password if I'm using a public WiFi since you mentioned my data will be collected when I'm using the campus WiFi. I know there probably will exist sort of network security protocols, however I still get a kind of unsecured feeling.

Online payment, need pin of credit card

Apart from registering, I wouldn't like to do any extra thing



4/4

After you have answered all the questions above, do you agree to share your answers for research purposes? All the answers will be anonymous.

65 responses

- ● I chose 'I agree' at the beginning. Now I still agree.
- ● I chose 'I agree' at the beginning. Now I don't agree.
- ● I chose 'I don't agree' at the beginning. Now I agree.
- ● I chose 'I don't agree' at the beginning. Now I still don't agree.
- ● I don't remember what I chose at th...
- ● I don't remember what I chose at th...

You have completed all the questions.

Appendix 2
Generative session

real-time location (routine)	location at a certain moment	device using time (when?)	downloading behaviour (e.g. file size)	device using duration (how long?)	what kind of device (laptop/mobile phone)	what kind of website you visited

Your personal information is passively being collected via WIFI access points. All the information below is tracable. From -3~+3, please indicate how private the information is.

-3	-2	-1	0	+1	+2	+3
The information is not private to me. I'm totally ok to share this information.						*The information is very private to me. I totally disagree to share this information.*

Your personal information is passively being collected via WIFI access points. All the information below is anonymous, but can be traced as one user profile. From -3~+3, please indicate how private the information is.

-3 -2 -1 0 +1 +2 +3

The information is not private to me. I'm totally ok to share this information.

The information is very private to me. I totally disagree to share this information.

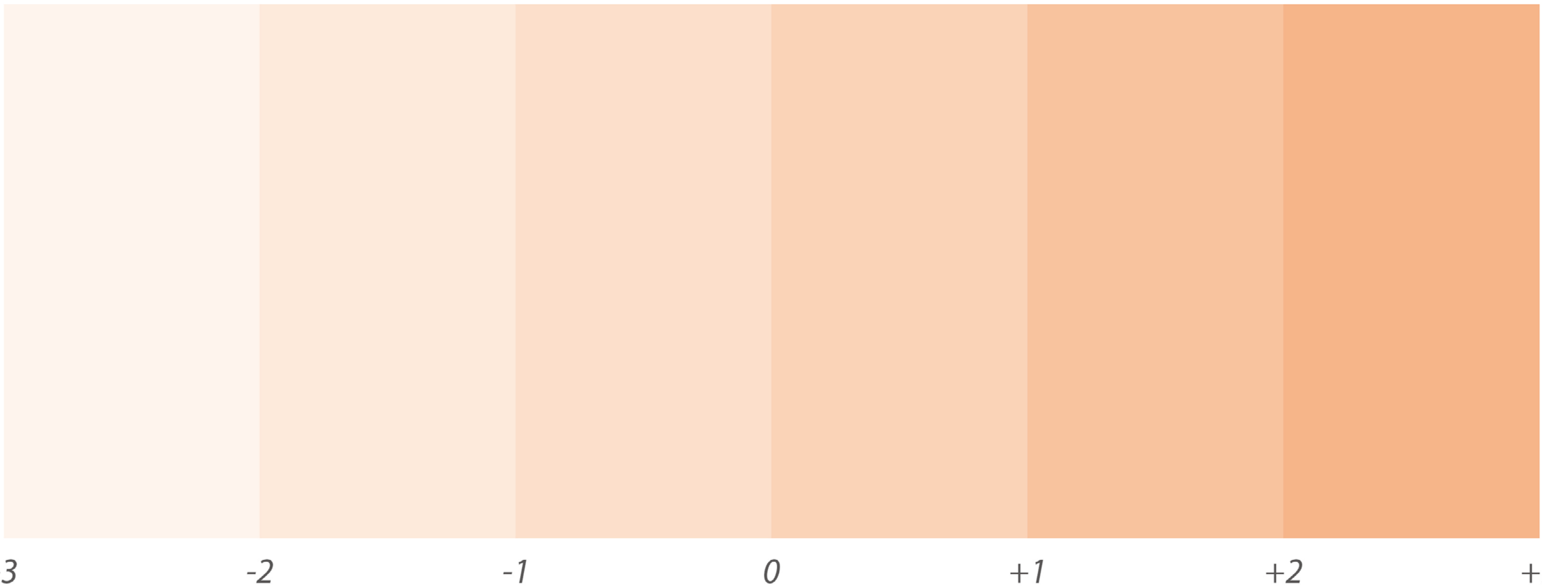
Your personal information is passively being collected via WIFI access points. All the information below is anonymous, non-tracable, and can only be studied as 'big data'. From -3~+3, please indicate how private the information is.

-3 -2 -1 0 +1 +2 +3

The information is not private to me. I'm totally ok to share this information.

The information is very private to me. I totally disagree to share this information.

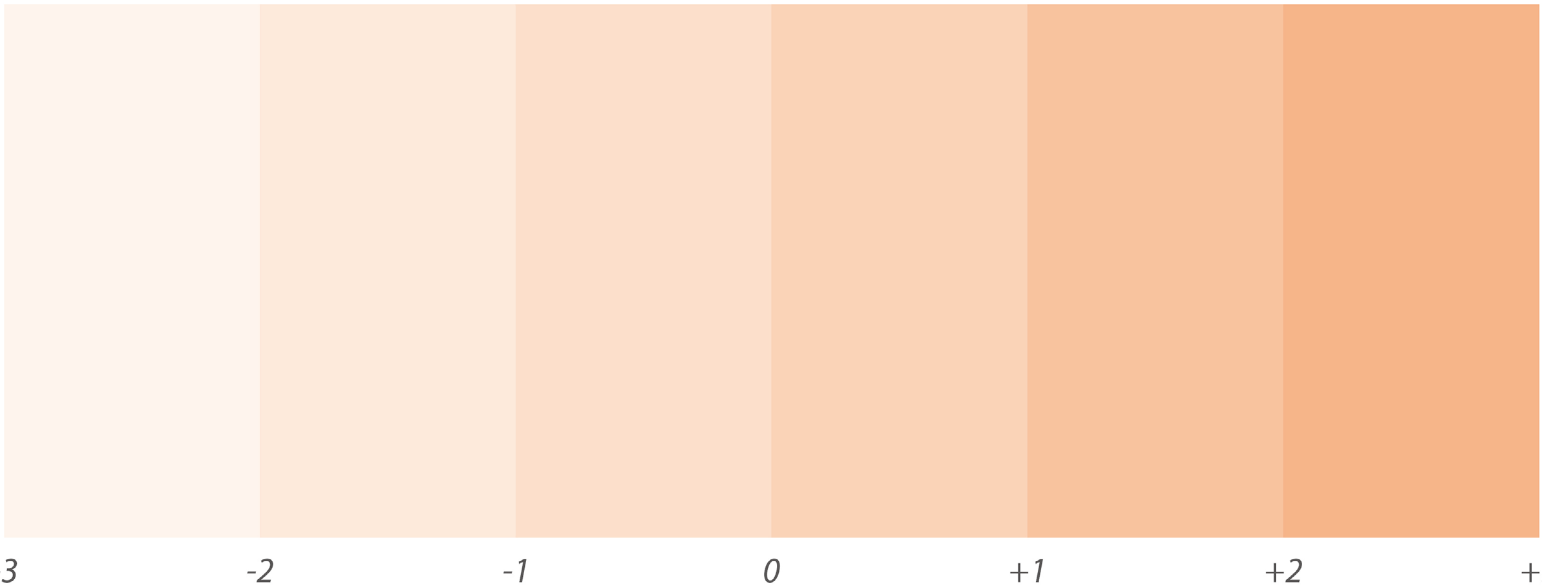
For better management of working space (e.g. Suggest students to go to other faculties when the library is full.)



I don't want to share my data for this purpose.

I'm very willing to share my data for this purpose.

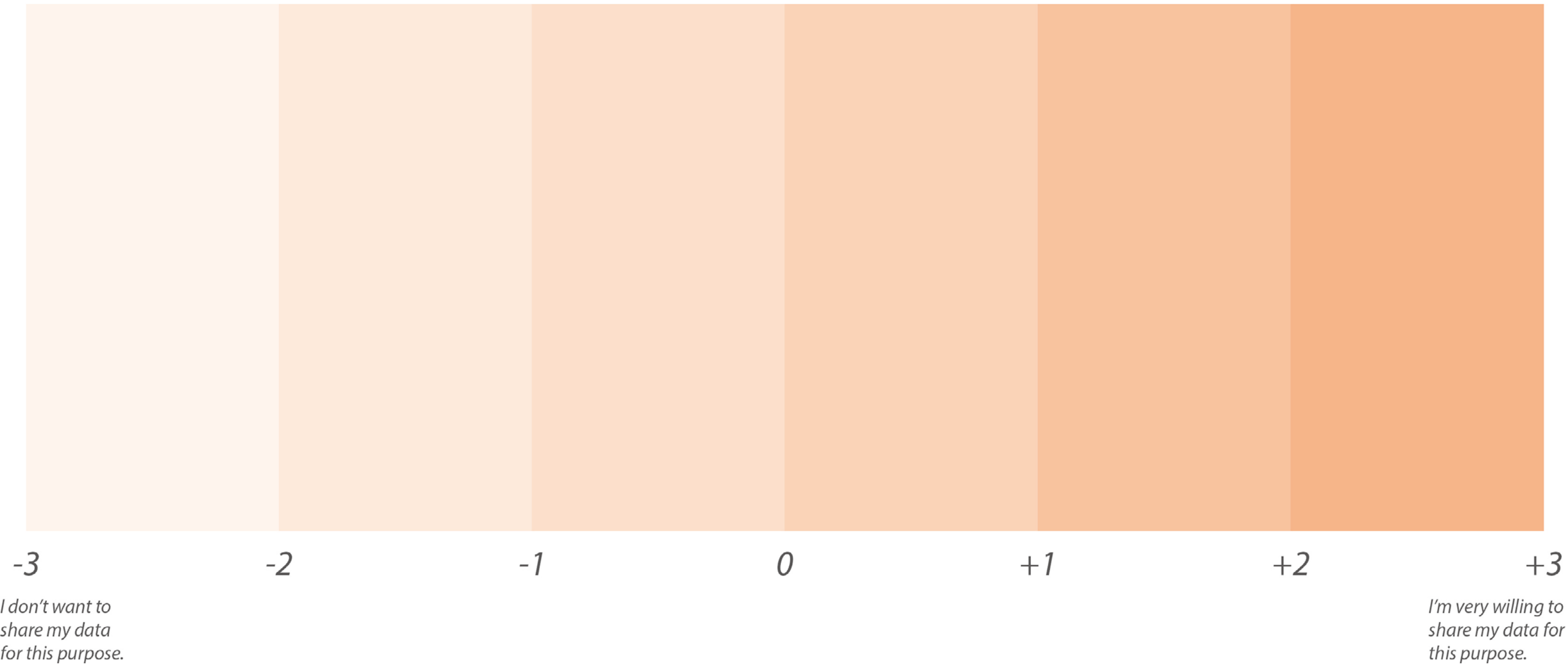
For better management of campus services. (e.g. Prepare more food on Wednesday because usually there are more people in Aula on this day.)



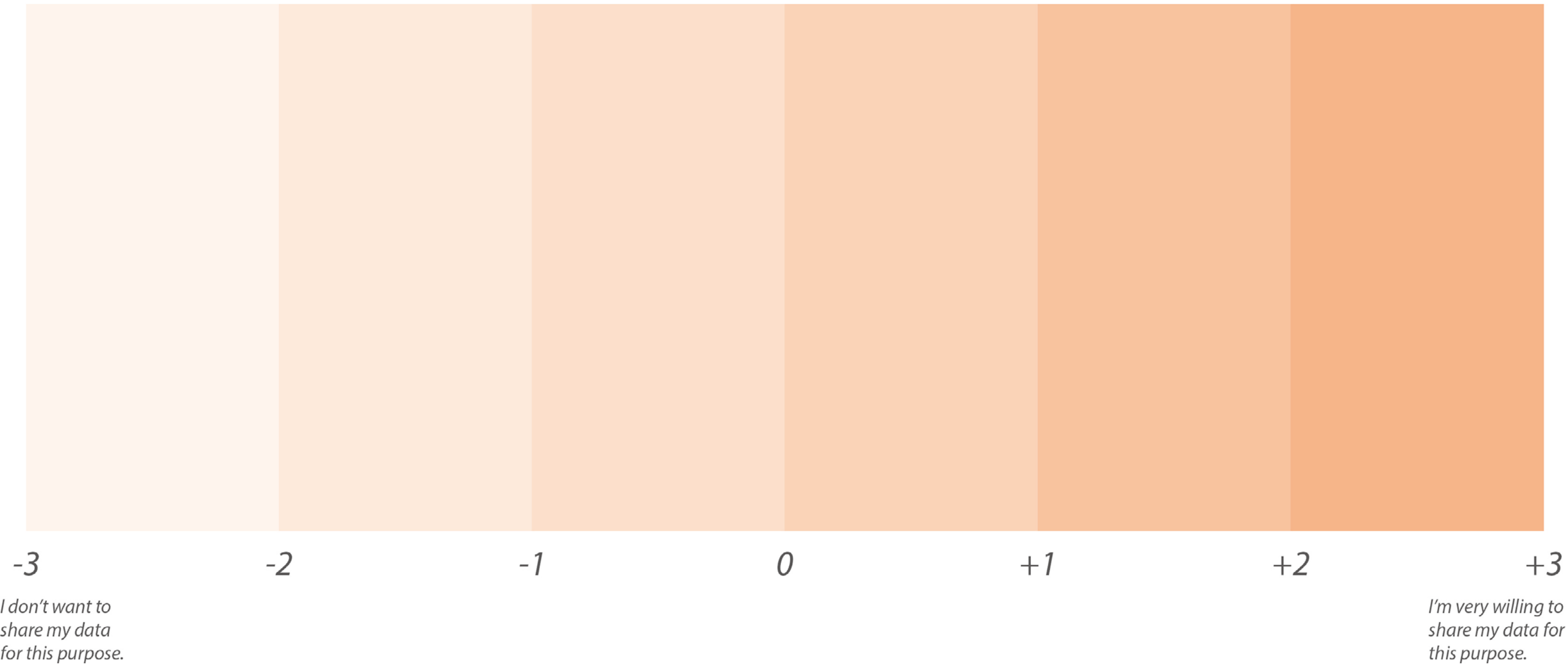
I don't want to share my data for this purpose.

I'm very willing to share my data for this purpose.

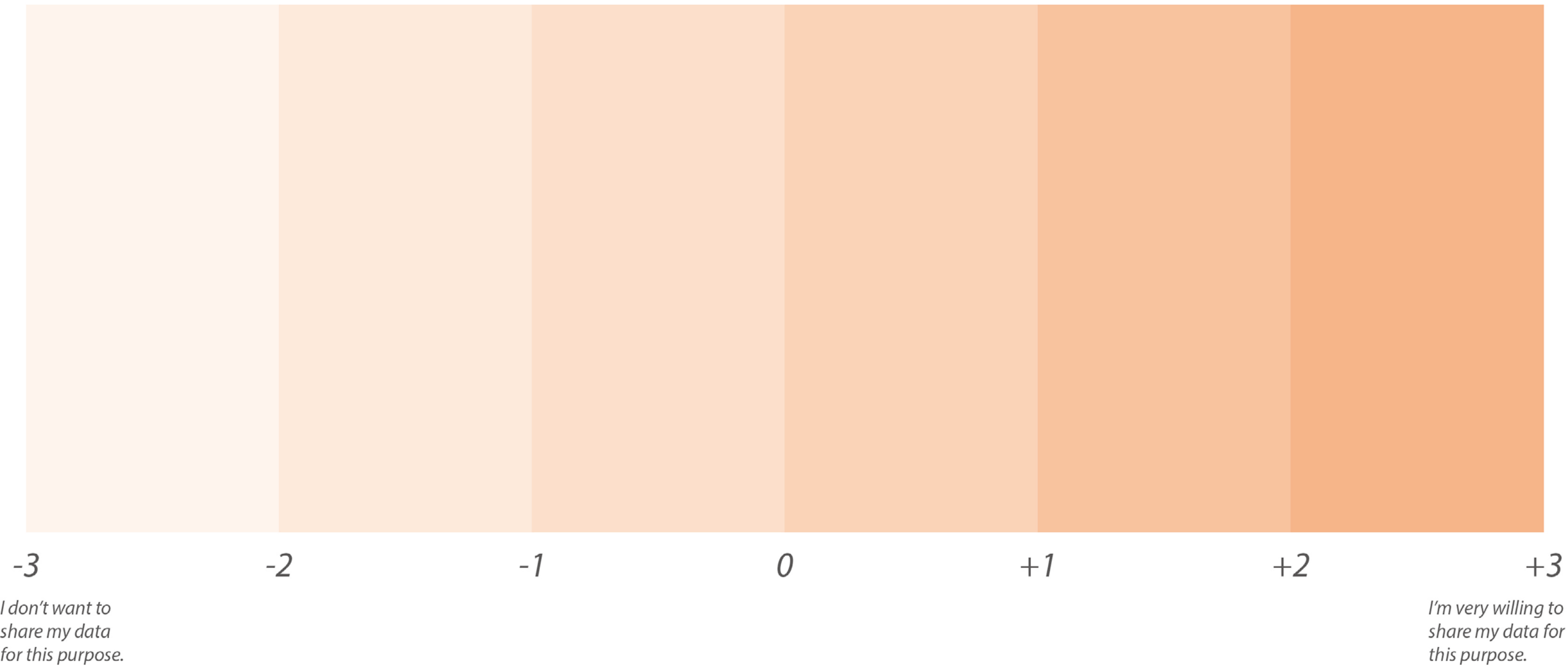
For emergency evacuation plan. (e.g. Design of the evacuation route in the building.)


-3
-2
-1
0
+1
+2
+3
I don't want to share my data for this purpose.
I'm very willing to share my data for this purpose.

For improving campus internet service. (e.g. setting up a cache server which maintains the most frequently visited resources in a period.)


-3
-2
-1
0
+1
+2
+3
I don't want to share my data for this purpose.
I'm very willing to share my data for this purpose.

For all kinds of research purposes of the university researchers. (e.g. Studying students' behaviour patterns.)


-3
-2
-1
0
+1
+2
+3
I don't want to share my data for this purpose.
I'm very willing to share my data for this purpose.

Important quotes from generative session

Respondent 01

1. This data is okay for me if it's collected only in the campus. However, I don't want them to be collected elsewhere. Especially the browsing history.
2. If someone uses my anonymized data for research, I would rather be happy.
3. (Purpose 1) I don't want to share my browsing history. I don't know how it help improve working space management.

Respondent 02

1. Locating me is very scary, it feels unsafe. I don't want anyone to find me.
2. When I'm at home, I'll visit more private websites. In the university it's less private.
3. I don't think what kind of websites I visit is relevant to this purpose [managing working space]. My intention of sharing data is totally based on how much this kind of data contributes to the purpose.

Respondent 03

1. All kinds of data are important to me. I care about my privacy a lot.
2. [Condition 2] Even though they don't know my name, they know it's a specific person because everybody has a pattern. So it's the same to me whether they anonymize my data or not.
3. If they want to use the data for some good purposes, then I'm willing to share some not-so-private data.
4. GDPR gives me a feeling of security.
5. [Improving Internet service] I don't really believe these data collected can help this purpose.
6. If you tell me your purpose of collecting my data, I'm willing to share.

Respondent 04

1. Even it's totally anonymous, I don't want others to know what kind of website I visit, and what I download. I don't trust them.
2. [Working space] I don't think for this purpose they need my data.
3. I'll feel more assured if you tell me the purpose of using my data.

Respondent 05

1. [Condition 2] Even those data are anonymized, if you analyze them all together you can still tell what kind of person it is. It's dangerous.
2. Location is the most relevant information to personal safety, so it's the most private.
3. I especially don't want my browsing history to be connected with my location. For example if I view parenting website a lot, you can imply that I'm a young mother. Then if you know my location, it's not safe for me.
4. If it's the university who wants to use my information, I'm not that worried actually. I worry that the information might be leaked.
5. What kind of purpose you want my data for doesn't affect me a lot. If I don't share my information, you can still use other people's.

Respondent 06

1. Even though they can only see the file size of my downloading, I still feel uncomfortable.
2. To me, condition 2 is even worse than condition 1. In condition 2, you tell me it's anonymous, but still you can imply from my routine and browsing history, you know it's me. If it's condition 1, I know it's real name so at least I'm prepared.
3. If it doesn't affect my real life, it's okay.
4. [Working space] It's not that I don't want to share my downloading behaviour. I just think it doesn't help.
5. The real-time location is to precise. I still worry about it.

Respondent 07

1. [Condition 1] I'm afraid that my device information be sold to third party. For example, an salesman might call me to sell Apple device.
2. [Condition 2] The anonymized information won't affect my everyday life. But if someone tries to reach me with those information, then it's the same with Condition 1.
3. It's in the university. I trust it more than other companies.
4. [Campus service] I don't think my device information is relevant.
5. The location data is okay. I'm not a very importent person. I don't think anyone wants to follow me.
6. [Internet service] The Internet service, it seems I don't have a choice... Okay, let them know. Though I don't want to.
7. [For research] Though I'm still not that willing to share, it's for research, okay, I'll give it a higher grade.

Respondent 08

1. All the content information are very personal. The university shall not know about it.
2. The location is inside the campus anyway. It's not personal.
3. I have a clear distinguish between personal and public things. Device information is definitely my personal thing. If it's the school's device, I don't care about it at all.
4. [Condition 2] Even though it's anonymous, they know it's one person. So no big difference.
5. The browsing history is not only private, it's also unneccesary.
6. If I download a file and it's big, it might raise other's curiosity.
7. Comparing to real-name, I'm less willing to share my location in Condition 2. You anonymize everything, and then you connect all the information to one person. I doubt your intention in this situation.
8. [Condition 3] The duration and location information as big data... Then I'm not 'okay' to share those data. I'm 'willing' to share them. Because it's the university, I believe they have a good intention, they will use our data for campus management.
9. If you don't ask me for this data, I won't voluntarily give it to you.
10. I do hope I share the most relevant data. If you ask for my data that's not so relevant, I will doubt your purpose.
11. [Evacuation plan] Any data that helps could be shared.
12. [For research] The purpose is not clear. It feel like "I want to do something today. You have to help me." You want to do a research, okay, it's none of my business. I want my data to be used to help others. You don't tell me what it's used for, so I don't really want to share.

Respondent 09

1. My device can reflect my financial status and brand preference. It's kind of private.
2. Browsing history is more private than location.

Respondent 10

1. Location is closely related to my personal safety.
2. If I download something really big, will my data flow be limited?
3. [Working space] Because you tell me the purpose, and it's meaningful to me, so I'm willing to share.
4. [Campus service] This 'campus service' doesn't sound clear to me.
5. I don't know why this device using duration is useful. I think the exact using time is more important than the duration, because you can see the peak of number of users.
6. [For research] It sounds a bit vague. What's your project? What are you going to research? So I won't share something specific for this purpose.

Respondent 11

1. Most of the time when I'm in university, I study. So I don't care about these.
2. I can't think of any situation I don't want to tell others my duration, because everyone connects to the Internet at the campus.
3. My only concern about the data is someone who knows me look at my browsing history. I feel uncomfortable.
4. [Working space] If sharing data does not affect anything, I would like to share. If it does, for example, I cannot study in the library if I spend too much time on social media, then I wouldn't share my browsing history.
5. I'm not sensitive with my information. If it doesn't harm me, I can share it. But I would like to share more important information if possible.

Respondent 12

1. Even it's 'big data', I still wouldn't share my browsing history.
2. Device is not privacy. Duration isn't either.
3. The real-time location kind of has a feeling of following me. But it doesn't matter.
4. [Working space] I think browsing history won't help at all.
5. [For research] If I'm not interested in the research project, I don't want to share.

Appendix 3
Expert interviews

Interview with Lolke Boonstra

W=Wang, the interviewer
B=Boonstra, the interviewee

W
Maybe I have to give a brief introduction to what I'm doing now. I'm doing my graduation project with Jacky. And we are researching on the topic How does the wifi access data influence the privacy sensitivity. Ok. Now the context is that with the GDPR being carried out, the researchers might have some problems accessing to those data. So I want to know if they are facing any problems, and how can we solve this problem. And at the same time, how do the student, employees, who are the data providers, how do they care about their privacy? Do they mind if their data is being accessed by researchers? So we're looking at this whole context to see, how do they feel like?
I know that you are the ICT research expert in our school. So can you give me a brief introduction of your daily work?

B
Oh, my daily work. [laughs] Uh, currently, as you said, I'm now doing the ICT support for research, uh, talking a lot about how to do the support and and finding out what is missing.
Yeah, we're in a very small group. We are with uh, just one colleague.

W
So you are two?

B
Yeah, we are two. We cannot implement things a lot by ourselves. We are relying for implementation of solutions. We still have to rely on ICT operations. Ok. And they're pretty busy.

W
They're pretty busy. So how big is this ICT department?

B
The department is very big. Uh, the whole department operation is about one hundred fifty people. Yeah, I am in what is called the ICT Innovation Department and it’s divided in the research on education.
And the innovation department is only eight or nine people, to do the research part.

W
Ok, so the others are all technical people?

B
No. Uh, yeah, the operations are all technical. When i'm talking about ICT operations, that's the people who maintain the network, the storage, the systems, and things like that. And maintain all the business applications and doing things like all the print. That's good, yeah.

W
So you are working for ICT Innovation.

B
Yeah.

W
So how does your work helps the ICT department, or help the school?

B
We're doing the ICT support for researchers. So we want to help the research with ICT demands.

W
So if a researcher wants to come to the ICT department, they come to you. Is that correct?

B
Uh, that's that's what we hope. [laughs]
Yeah, if you have a specific research ICT question, not on your file, mail, print, or the laptop is not working or whatever, or the network is not working. If they have special needs to do the research, special ICT needs to do their research.

W
So can you give me some examples of these ICT needs?

B
Uh, that can be special network connections, special storage. So everything which does not fit in the standard ICT things. And the standard ICT is basically just uh, it’s a business application, it’s just for having an office running. And that solves already seventy percent of the researchers’ need for ICT. Because, yeah, you have a network connection. You have at the moment a Wifi connection. And you have a connection to your personal storage on the TU Delft. If you wanted to do file sharing, if you want to print something, that's what you can do. But that's not what we do.

W
You're giving them special support.

B
Yeah, for example, we had some special network connections for four different use, uh,

research groups. Sometimes there are special needs for local environments. And then we have to see how that fits in the whole campus environment, which is that, up and running.
And what is at the moment we know what is missing. Yeah, the two things which start up now, for researchers, that's data management. That's what we do together with the library, we are busy with. And the other one which we have noticed is when there is a lot of requests for this software engineering. So that's a completely new field for for us.

W
So I think I have more questions with the data management part. You just gotta do. So, do you mean, data management, that they request data from you, or is there any kind of other requests?

B
Yeah, one of the main things I've been doing is our requests from the researchers on data, which the ICT department has. So then you come to the Wifi data and the network data, also part of it. Yeah, that's mainly the big ones at the moment.
And that's where ICT is also the owner of the data. And we also have the service for other buildings, which control cameras and which control the heating systems. And there's also a lot of data within that. But ICT is not the owner of the data.

W
It’s not?

B
No, no. Only the real estate is the owner of that data.

W
So who is the owner?

B
Real estate. Yeah, real estate, they’re the owner of that data.
So yeah and I have been busy with that. Just starting. I'm busy with just getting the ICT data more flexible available for the researchers. That's what I've been busy doing for the last two years.

W
So if the ICT is not the owner of the data, but are researchers requesting it from ICT?

B
No, no, no. We just do not do that. Okay. What i've done with that was just say, we are busy with creating uh, we want to create a data platform for researchers. The first thing we will put in there is the ICT data. Because we are going to create the platform as ICT. To get your own data in is easier than to get someone else’s data in. Once that's running on, that takes more time than I had expected. Well, we probably will also be discussing with real estate if they want to put their data in also.

W
Okay, so what is the value for ICT now? You say that they're operating the internet service in the school. So does it mean that what they care most is to maintain the internet service for our school? And that's all that's their main value.

B
Yeah, yes. Maintaining the whole ICT infrastructure. That's the main value. But there also should be a shift, to also shift more to ICT support for education and for research.

W
So you think there should be a shift to that.

B
Yeah. But that's in the strategic policy of the board. So we have to follow. [laughs] And that's what I hope that would be, because that's what I want to do.

W
So how does it work now? If for example, researchers or research groups want to have a certain database or something, is there any procedure that they apply for it?

B
No, there is no, not standard. Okay, no, it's just individual contact. Uh, why, uh, why things happened. And I already was busy, I have been giving data from ICT to researchers for a long period. I'm now working for ICT innovation for two years, before that I was working at operations and I have been giving the Wifi data and also netflow data to different users, to different researchers along. They know I'm busy with it. And if they want to have the data in that sense, they mostly know data, they know me, and they have been spreading around the words. If you want to do. That's why you're sitting here. [laughs]

W
Yeah. So you you talked about Wifi data and Internet data...or something like that?

B
Uh it's a problem with the word Internet. Network data, because it's just the data which is going around the campus. So I cannot see what's going on between Amsterdam and London.

W
So what kind of wifi data is there? Because I have some problems differentiating these kind of data. So for example, my browsing history, it is not wifi data.

B
Yeah, I noticed that. Yeah, of course, talking with Jackie and on a different subject, but still on the same subject.

The wifi data, uh, it's the technical data. And that means the data which the Wifi protocol needs to contact you, and that if you're moving within the building that you still keep connected, especially with your phone for most of the time. That information is called Wifi data.

W
When I approach a Wifi installation and something like the signal...

B
Yeah, the strength of the signal is known. Of course, your mac address is known. IP addresses known, and there's also your user credentials. Your username is known, passwords, of course, but not what you do.

W
Ok, so not about the content.

B
No. It's only about what's in a network terms, it is said, we never know about the payload. So yeah, it's just the technical information, and the communication from the access points to the central system where the whole Wifi is maintained.

W
So what can you imply for from those data? There are lots of researches going on about Wifi access data, like location information.

B
You can see that here around this access point, at least there are one, two, three, four, five devices running. And that probably means that there are two people sitting here.

W
Ok. So you can imply from it that how many devices and how far it is between the device to the access point.

B
Yes. And depending on how your place and your access point, you can do location based services, but it depends on how you give me triangulation for that. And you need to have clear borders on your building. And the way it is implemented here, at TU Delft, it’s not that easy to do location based services.

W
Why?

B
Because you can see all our access points on the roof, mostly you’re connected to the access point underneath your feet. And then the location will say you're on that third floor instead of your own fourth floor. Okay, so details, it depends on what you want to

do. But I know there is research going on the evacuation of a building. And they want to use the wifi data so they can see if the building is evacuated or not.

W
Ok, so they use it during the evacuation. So not predicting how people move, but during the evacuation?

B
And you can also see how people move. That's what you can see. That's what you can usually see the movement of a device, still device based.

W
So that means that you can see the real time location of every device?

B
Yeah, but keep in mind, it's device based.

W
So is there any kind of privacy issues?

B
Yeah, because the unique identifier of your every device called a MAC address is in that data.

W
So the MAC address is encrypted?

B
The legal term for that is pseudonymised. It's not anonymised, but pseudonymised. If we give data to the researchers, we should pseudonymise the data.

W
But technically, you can recognize every device.

B
I cannot recognize it's your device.

W
But when I log into the wifi, I have to enter my username.

B
But usually the username is not given to the research. That's what we anonymise from the data. But yeah, otherwise it would be very easy.
For maintaining, because the data on the maintenance platform is anonymised, is not pseudonymised at all. So, the people working at operations they can see everything you're doing. But they're not allowed to do that. Okay, so and they only are allowed to

do things if they are summoned to. Okay, so if the police is coming and they want to track down a person, the most questions are this IP address has been doing something, who was behind it up here that we can find it out.
But that's not our concern. The main thing is the legal difference. For operating, but you are allowed to store more data, more privacy related data. And there is a reason to maintain that completely privacy data.
So MAC addresses and IP addresses, which is privacy data.

W
Privacy?

B
Yeah, that's my definition. Otherwise, the wifi data would not have been a problem. But the law has said that the MAC address is the privacy. So they're protected by the law.

W
So they're protected by the law. So does GDPR actually change anything?

B
Not on that sense, because there already is the old law, the WPB already had rulings about how long you were allowed to store data and already said that MAC address was privacy data. So the GDPR did not change anything. The only thing happened on management level is changed a lot.

W
So can you give me some examples?

B
It is well known that the attitude after WPB was not implemented.

W
WPB is not implemented in TU Delft?

B
No. So what we are doing now is what we already should have done ten years ago.

W
So now you are implementing GDPR in TU Delft.

B
Yeah, that's what’s happening. And that's where a lot of people are discussing. Because there has been a lot of discussion on the GDPR, in the public also, which most of the time people say, but that should already have been done.
It should already have, it should have been done with the old law. In that sense, the GDPR did not change a lot.

W
But it actually changes something because the old law wasn't implemented?

B
TU Delft didn’t implement. So we are never old law compliant. I mean, we still can not implement GDPR.

W
Why is it, why can you not implementing it?

B
There was no one who was thinking that it should be, put in the effort, because it costs effort.

W
Is it legal if you don't implement it?

B
No.

W
But it doesn't matter?

B
Yeah. [laughs] Okay. But not implementing things is… that is really a bit cumbersome at the discussion about the GDPR. That a lot of things which I mentioned, should already have been done within the old law. So how long do you store the data, what data, and you already had to explain what you were storing. And that was never done. Yeah, but that didn't change with the GDPR.
The only thing which happens is that on management level, we have to do something. And we're now doing so.

W
So if GDPR is fully implemented in the school, what will change? Like, for example, the researchers want to access the data.

B
The only thing which would then change is that we have to write down how long data is stored and the change is also that we no longer store it in, definitely, which we did.

W
So is there any problem for the researchers? Because that's what I'm working on. So i've heard that if you want to research, you have access to those WIFI data, does it mean that everybody who uses this wifi have to give their consent that they allow?

B
No, that's not for the research platform, because I did not want to use the consent direction. There are different ways to have legal grounds to store privacy data. And the beautiful thing that's called research is a legal ground to store data.
And that's the ground where the data platform which we are creating, and the data which is collected because of operations. That's the legal ground for having the data moving to the data platform. That's done on the legal grounds doing research. And it’s making it hard because for you and for your research, because no, you're not giving consent for the Wi-Fi data as an individual. And we're not asking for it.
At the current state, that is allowed. And that is what I'm aiming at with the whole data platform.

W
So why do you keep talking about this platform?

B
Because that's making the difference in the legal grounds where you are allowed to store the data, because this is only storing the data for research, then still the researcher has to do a request to get the data out of that platform, and still has to create a document saying what the data is used for, and also probably the most legal ground I would do as a researcher is doing it because you are doing research, and that's why you can take the data out of the platform for yourself and store it again somewhere else, because you probably will store it against someone else, because also this data platform as a short period of storage.
Ok. And for research, you have other rulings on storing the data, on how long you will have to store your data.

W
I don't know if I understand it correctly. Now you store the data and you want to create a platform which you can move the data to your platform, where all the researchers can have access to.

B
Ok, that's because you don't want the researchers to connect to the operation, that interference you don't want.

W
So why do you think you are not uh, working towards the consent direction?

B
Because it's no way I can get consent from everyone in the university and filtering out you is pretty hard, because as soon as you get a new device, you have to tell me that it's you. I'm not filtering out you, I'm filtering out your devices.

W
That's interesting.

B
And that’s the Wi-Fi data. And if you take the network data, I'm not filtering out you, I'm filtering out your IP address. And your IP address is changing, it’s not the same every day. And you are an Industrial Design student. If a TPM student comes here, their IP address is different from here. And there is a possibility that you still have the same IP address.

W
It’s complicated.

B
Yeah, yeah. [laughs] When I started creating this and data platform, I started it as a technical project. I am security minded and ethical minded, but I want to do in an easy and the most pragmatic way. So I was saying, okay, let's talk to the ethics committee about this whole thing. And also and I already had some contact previously with the old law, with the legal department on giving data away. And that was no problem at all. And when I started with the ethics committee, they were like but we have to think about consent. But no, that's not the direction I want to go.
And yeah, it ended up in a completely discussion on all the ethical and legal things. I have organized a workshop on that. It's already, I think, a year ago on the whole legal things concerning this platform. And then that's where I came out with the division into the three parts. You have the you have the source, you have the producer, and you have a consumer, and all three should be GDPR compliant.
I don't bother about the source. That's something operation has to do. I was bothering about the producer side and the researcher has to bother about the consumer side.

W
Ok, so who are the consumers?

B
The researchers. And what we are now thinking of, that we probably will make some standard consumers. So, but I understand the template. The researcher still has, in every research, if they are using data, they have to tell if the data has privacy, is there sensitive data in it? And if so, how they're gonna deal with it.

W
So they have to think about it instead of you have to think about it?

B
I also have to think about it, from moving the data from the source to the platform. And then I have to tell what date I'm going to take in there. And there is privacy information and so. And I have to tell what measures I have taken? That's called DPIA, and you must have DPIA for all the three, so for the source, producer and for the consumer.

W
So what's the whole name of the DPIA?

B
Uh, I never know where the D is for, but P is for privacy, and A is for assessment, privacy impact assessment. And that's where you tell, that's just, the first question is do you have privacy sensitive data? And within your data set where you're working with, if yes, then the next questions come into our mind.

W
I'm sorry. I'm a little bit forgetting this. So you have the whole operation, you have the researchers. So who is in the middle?

B
As I said, I use the terms source, producer, and consumer. And the source at the moment is now ICT. The producer is ICT and consumer is researcher. In the future, the source can be Real Estate and producer will still be ICT. Okay, so that has to do with who's responsible for as I said, Real Estate has also very interesting data for researchers.

W
Ok. So can you tell me more about this Real Estate?

B
Those are the ones who built the buildings and are responsible for the heating and electricity and things like that. And they have measurements on, especially in the new buildings, on how much oxygen is in the rooms, how warm it is. That's all kinds of data which resides on the systems. They run to have this climate control.

W
So they have all the hardware here. So that's why they own the data?

B
They are owner of the building systems. Then your problem is, does system run on surface, which are, of course, maintained by ICT. But yeah, that's the same with the maintenance system of the Wi-Fi, it’s also run on surface. But that the dimension system of the Wi-Fi is the responsibility of ICT. The maintenance system of the buildings is responsibility of Real Estate.
And what you are now seeing the with all this internet of things going on with a lot of sensors, and this location based services. There for real estate, it is very interesting to know if a classroom is occupied. And that's where you can use Wi-Fi data for a little bit.

W
When I was doing research, I found that three or four years ago there was a course or a track running on civil engineering faculty and use the Wi-Fi access data to study student patterns in Aula and library. So I tried to contact one of the master students at that time. And he said that, when they were doing this project, they didn't have access to the eduroam data. So that's why they installed their own Wi-Fi installations.

B
Yeah, that was also...which tracks the things we have given to other groups. There's also students at computer science who have been working on that and they got access to eduroam data. And the things they create with is seeing how people move between the buildings on campus. And they also did tracking of MAC address, see how that one was moving on the campus.

W
So it is allowed to give the accessibility even to the students?

B
It's always given to employees, but there is an employee who is responsible for the solution. And it's given to a person who is responsible for it. There is also a responsible employee for the data. And I expect that also bachelor students are very aware of handling data correctly. If you don't do it, what would happen? I don't know. [laughs]

W
Yeah, Jackie told me that the school is selling or bidding some of the data. Is that happening?

B
No. All the data and all the data sets which has been created in the last decades is open data.

W
Open data?

B
Yeah, it’s even open data. Because I know that it's now already, I think more than ten years ago, I think already fifteen years ago I've given away a data set for research on network data, for research on security algorithms. And that said it’s used in some publications. And I have told, like any research that the data set should be available for everyone. Because we never did a restriction on it. And the researcher who worked with it has now a company called Radically Open Security. So she is very busy on doing things in open science and open data.

W
Okay, tell me more things about open data, like, what's the standard for those open data and who can access to those open data?

B
That's not my responsibility anymore. What I'm saying is the researchers are not allowed to sell it. And I think that the research is allowed to publish it openly.

W
But what about, for example, Real Estate, if they want…?

B
Because I'm not talking about the data from ICT because first we start with it and see how that will happen. Because the Real Estate data depends on what you're looking at. Because Real Estate also is responsible for all the cameras on campus, and that's not the data you want to share. That's the difference.

W
So does it mean that every data being collected is under the law protection, or is there something that is not defined as private data, so you can do anything?

B
No, all data which ICT collects for operation, almost everything has privacy, because all unique identifier has privacy elements. So as soon as you create a database, there is a unique identifier.
So on the source side, there is always something to do. And that data is never stored in an anonymised way except for passwords. Profits are always stored encrypted.

W
I think I've asked most of the questions. So one final question. What are your values when you are doing your work?

B
What drives me is to get the researchers doing better research.
And if I can help them with data sets, then I will help them. That's how I started giving data sets to researchers. And they had sometimes the questions come along. And I think, yeah, this we should, in my opinion, you should always help the researchers. It is that has changed also with the whole GDPR. Other companies are more reluctant to give away open date.

W
Why?

B
I think it's from fear, because there was a lot of fear created with GDPR. Because it said about fines, which you could get if you're not GDPR compliant. But fining a university with millions of euros, this will never happen because we're not able to go bankrupt. [laughs]

W
That's true. It's easier to do in the universities.

B
Yeah, because they're fining a university, it’s where the government is also one of the main supplies of the payroll. That does not work.
Of course, if you do something terribly, completely wrong, if your student administration is so wrong, using the wrong, doing the wrong things or you use administration, if you

store your passwords still in an unencrypted way. Ok, then... but that's, if you use or if we would use unique identifiers, which you're not allowed to. That's what the Dutch tax has been doing, they had used the unique identifier of every person for a different case. And that was not allowed. So they are.
But then still you get the time to solve that problem. And that is at least half a year. And if you have done your legal ground well and it's just paperwork, that's mostly paperwork, and then the legal people have to make some rulings. So what's not allowed, or what's allowed?

W
Do you have any difficulties when you want to help the researchers or anything like that? Any troubles?

B
Yeah, for me, the most problem is getting resources to implement things. That's justin internal part.

W
So what kind of resource are you talking about?

B
Creating the platform, having people install program. Configurating and programming. That's where I hope Jackie will help also.

W
Okay, I think I've finished. Let me write this down. Thank you.

—— Chatting after the interview ——
B
The implication of GDPR is there is a lot of work to be done on what I called that should be done in last 10 years. The universities that already implemented the old law very good and very detailed, they don't have any bad with GDPR. On the other scale, the ones who did not implement GDPR and the old law now have a big job, they now feel that they have to do more. That's why ICT has taken responsibility for some legal things, we hired in some legal processes to keep the whole GDPR compliance up and running.
What to do with the researchers? The whole process for researchers to undertake, that they have to be GDPR compliant, be ethical compliant, have a good research data management plan. The process, they want to investigate that, and hopefully to standardise that, and to automatic it. It's now the burden for a lot of researchers because of those three things, can be a lot of job to do. The implementation is more on being compliance, that means the paperwork is done correctly.
And if you have a research proposal, you have to make it GDPR compliant, you have to have research data management plan, and that work is still not…if you don't do it, there's no penalty on it, but that should be incorporate more in a standardised process. And that's where we're doing ICT support for research. Together with the library we do the investigation, with ethical committee we investigate on how the processes are.

W
So is ethics committee monitoring on requests from researchers to ICT?

B
If you are using data sets with private data in it, you must pass the ethical committee. I don't think every researcher is doing that. [laughs] They should, but as I said, if the ethics committee is not told that there is a research going on, then they can't check it. Nowadays all the research proposals need to have a data management plan, and need to be GDPR compliant. It is all "should should should" and if you don't do it, it's not checked. But keep in mind that all bachelors' research must go through that process. That's too much. We first start with big projects and PhD projects. But there's nobody knowing what research projects are in the whole university. I don't even think on the faculty level the faculty knows all the research projects.

W
That's true.

B
So there's no checking, because there are a lot of research projects that are never known, because no funding needed, so there's no internal code for them. Then there's no way for checking.

W
On your dream platform, who will do the checking?

B
For the Wi-Fi data producer, I already did the paperwork. But it's just paperwork. I think it was the first privacy impact assessment created for the whole TU.

W
That's cool. But I thought the Wi-Fi data is less private than the network data. Is that true?

B
No. They are the same.

Quotes from interview with Edward Verbree

1. If you would like to do any indoor navigation, then you should know where people are located inside the building. The method you can do so is using the Wifi data, because the GPS signal is poor inside the building.

2. Wifi access point are there to transmit data. Wifi is available everywhere. You can use that already. You don't have to do anything, and it's free.

3. Your smartphone can be detected by the access points around it. So you can use that information in a way to estimate your location.

4. But you can also do that in a way around. You can use that access point to see which devices are around.

5. If my device searches around for Wifi access, I can get a list of access points. That list of access points are more or less unique for this location.

6. I don't have to connect to the access points, I only have to access them. They're different, and it's important. If you look at GDPR, if I just scan with my device to see which access points are there, I don't have to connect to them. It means that I don't connect to them on purpose, I just approach them.

7. When I access different points, I not only get the list of access points, but also signal strength. So these access points are near to me, they are 'louder'.

8. If I apply the method *Wifi Fingerprinting*, it means a specific list of access points and signal strength. Then I link this list to my current location, and I create a database of my current location with this list.

9. Then I can also do it the other way around. I've created this list, then I choose the database which location do have these sets of access points. Then you can find out of that you are here.

10. I'm locating myself by doing so, there's no one else involved. When I'm building up that database, I know my current location.

11. The blue dot in Google Map shows your location. It's either be done by GPS, it can also be done with Wifi fingerprinting. It means I scan around the Wifi access points around me, and send that information to Google. During this process, I'm only using the Wifi access points, but the ICT department or people who own the Wifi are not aware that I'm doing this. So I can know my location without their awareness. And I can provide

my location to others.

12. With GDPR, that means I give my consent to Google to use my location.

13. If I am connected to eduroam, my device is connected to one of the access points. So if the ICT department know where the access point is, if they know the MAC address, and they have a map of all their access points, then they know this device is very near to the access point.

14.The ICT department is collecting the data to provide Internet service. They moniter the number of users to provide enough access points.

15. The ICT department doesn't collect our data. They only collect the number of users and MAC address to make sure that the distribution of access points is enough.

16. The researchers do know that they can use the data to study how many people are around an access point, how do they move and what's their behaviour.

17. The researchers just ask the ICT department for those data.

18. MAC address is a unique identifier for each device. If you know where the device is, then you know where I am.

19. Is the data anonymous? Yes, and no. If you can make a relationship between a MAC address with someone who is working in this building, you know that I work in this building, then you know that the MAC address is me.

20. I can only be connected to eduroam with my NETid. That contains my login details. My MAC address and my NETid are stored together. But the ICT department will never ever give that information.

21. ICT will never ever give away MAC addresses. They will do some hashing, they will delete some data, before they give the data to the researchers. They only provide encrypted MAC address, so you can never ever refer back to the MAC addresses. So you only know that it's a specific device.

22. If I'm going to kill someone, and the police would like to know where have I been at this moment and time, then they will provide all the information to the police. So it depends on who want the data.

23. For research, I only want to know how many people are around here.

24. The GDPR has set some regulations. But when you're doing research, research is a very good reason to provide data. So the GDPR doesn't affect research a lot.

25. If I only want to know YOUR location, then I have to ask YOU. But if I want to study a

group of people, I don't think I should ask, but I'm not sure. It's a bit of grey area.

26. If I want to study a group of people, but I don't know who they are, so I can't ask each individual for consent.

27. But still, if I detect a group of people inside this building, and I do know who are the employees over here, so I can still connect a group of anonymous people to them.

28. It's a private matter if I can refer back to the people I know.

29. If you install a monitering Wifi device, you only count how many devices are around that access point without knowing the details.

30. Even if the data is anonymous, it's still a private matter. Even before GDPR, it's already an issue.

31. The data providers are not aware of the private issues. The researchers raise those issues. Either you have to raise the issues with data provider, to tell them we are going to use your data, maybe there are lots of works with legal department over here because of lots of regulations, or you can also walk around it. For example, to use our own Wifi equipment. To use your own equipment has some problems, for example, you don't have full coverage over the campus.

32. The ICT department doesn't allow you to install your own Wifi equipment, because it'll interfere their own setup.

33. The ICT department only cares about providing Wifi access, it's their job.

Quotes from interview with Balázs Dukai

1. When your device is connected to the access point, a login entry is created. By default, the log isn't saved. But for our project, the ICT turn it on to collect the data. For our project, they collect the data from the whole campus for one year. Then they continued, because this project shows that there are lots of interesting subjects to explore.

2. The main purpose of our project that uses Wifi data is to optimize the usage of the facilities. Because the facility management find more pressure with more and more students.

3. I don't know exactly who initiated the projects. The teachers who organize the projects find the clients, and one of the clients is facility management department.

4. Another group was able to identify a particular person with his movement data in the campus, but only with extra information.

5. And it's not difficult to find out a teacher's MAC address. Because the timetable is usually open, so your MAC address will move at a certain time and location.
6. The current procedure to get the data is quite informal.
-"Let's do it." -"Ok let's collect the data then."

Appendix 4
Value-centric quotes

The ICT department is collecting the data to provide Internet service. They moniter the number of users to provide enough access points.

The ICT department doesn't collect our data. They only collect the number of users and MAC address to make sure that the distribution of access points is enough.

The ICT department doesn't allow you to install your own Wifi equipment, because it'll interfere their own setup.

The ICT department only cares about providing Wifi access, it's their job.

We want to create a data platform for researchers. The first thing we will put in there is the ICT data. Because we are going to create the platform as ICT. To get your own data in is easier than to get someone else's data in.

Maintaining the whole ICT infrastructure is the main value for ICT. But there also should be a shift, to shift more to ICT support for education and for research. That's in the strategic policy of of the board.

There is no standard to get the data now. It's just individual contact.

The MAC address is encrypted when we give the data to the researchers, but technically you can recognize every device.

GDPR doesn't change a lot of things here, because of the old law. The old law already had rulings about how long you were allowed to store data and already said that MAC address was privacy data.

To implement GDPR costs efforts.

I don't want to use the consent direction. There are different ways to have legal ground to store privacy data. And research is the legal ground to store data.

We are creating a platform. We want the data collected for operation, which is the legal ground to have the data, to move to the data platform, for the legal ground to do the research.

We are not asking for your consent to give Wifi access data.

This platform is about the legal ground why you store the data. The researchers still have to request the data out of the platform, creating a document, saying what the data is used for. The researchers will probably store the data somewhere else, because the current data platform has a short period of data storage.

This platform helps the researchers not to interfere with ICT operation.

There's no way I can get consent from everyone in the university. And filtering out you is pretty hard. Because as soon as you get a new device, you have to tell me that is you. I'm not filtering out you. I'm filtering out your device.

Wifi access point are there to transmit data. Wifi is available everywhere. You can use that already. You don't have to do anything, and it's free.

For research, I only want to know how many people are around here.

The GDPR has set some regulations. But when you're doing research, research is a very good reason to provide data. So the GDPR doesn't affect research a lot.

If I only want to know YOUR location, then I have to ask YOU. But if I want to study a group of people, I don't think I should ask, but I'm not sure. It's a bit of grey area.

If I want to study a group of people, but I don't know who they are, so I can't ask each individual for consent.

It's a private matter if I can refer back to the people I know.

The data providers are not aware of the private issues. The researchers raise those issues. Either you have to raise the issues with data provider, to tell them we are going to use your data, maybe there are lots of works with legal department over here because of lots of regulations, or you can also walk around it.

The main purpose of our project that uses Wifi data is to optimize the usage of the facilities. Because the facility management find more pressure with more and more students.

You can imply how many people are around an access point. You can imply the location of the people. You can see if the building is evacuated or not during an emergency.

You can not only predict how people moves, but can see the real-time movement.

For research, you have other rulings on how to store the data, on how long you store the data.

The main purpose of our project that uses Wifi data is to optimize the usage of the facilities. Because the facility management find more pressure with more and more students.

I don't know exactly who initiated the projects. The teachers who organizes the projects find the clients, and one of the clients is facility management department.

Another group was able to identify a particular person with his movement data in the campus, but only with extra information.

And it's not difficult to find out a teacher's MAC address. Because the timetable is usually open, so your MAC address will move at a certain time and location.

The current procedure to get the data is quite informal.

-"Let's do it."
-"Ok let's collect the data then."

I’m afraid my device information could be sold to sales company. I don’t want any salesman to call me. For example, I use Apple device, but I don’t want any Apple advertisements.

I don’t want to share my viewing history information for managing working space. It’s not a privacy matter. I don’t know why they need this for that purpose. I rate my willingness only based on relevance.

As long as the purpose is being explained to me, I would like to share my data.

I still don’t want to share my location information. But since it’s for research purpose, I would put it [the location card] a bit more in the middle.

I’m actually not that worried that my information is being used inside the university. I just fear the information being leaked.

If someone use my anonymous data for research, I will be very happy.

If it’s for good purpose, I can share some information that is not so private.

My willingness to share my information only are based on relevance between my information and the purpose.

I clearly distinguish my personal matters and public things. For me, what kind of device I have is a private matter. If I use a school computer then it doesn’t matter if they collect my device information.

Comparing to real name, collecting my data anonymously and analyze it as a specific person is even more weird. I will doubt its intention.

I’m not ok to share my data as ‘big data’. I’m more than willing to do so. I believe the school has good intention, and it will be used for campus management.

Yes, I can share my data if it’s anonymous. But if you don’t ask me for my data, I will not voluntarily share it.

I want the researchers use my data to help others. But if you just tell me it’s a ‘research’ with no more details, I won’t share my information.

My device information might reflect my financial situation and brand preference, it’s very personal.

I don’t do bank transfer using eduroam, because I think the public Wifi is not safe.

As long as they only use the data for non-profit research or improvement of the whole service, I am fine with that.

If you would like to do any indoor navigation, then you should know where people are located inside the building. The method you can do so is using the Wifi data, because the GPS signal is poor inside the building.

Your smartphone can be detected by the access points around it. So you can use that information in a way to estimate your location. But you can also do that in a way around. You can use that access point to see which devices are around.

If my device searches around for Wifi access, I can get a list of access points. That list of access points are more or less unique for this location.

I don't have to connect to the access points, I only have to access them. They're different, and it's important. If you look at GDPR, if I just scan with my device to see which access points are there, I don't have to connect to them. It means that I don't connect to them on purpose, I just approach them.

When I access different points, I not only get the list of access points, but also signal strength. So these access points are near to me, they are 'louder'.

If I apply the method Wifi Fingerprinting, it means a specific list of access points and signal strength. Then I link this list to my current location, and I create a database of my current location with this list.

Then I can also do it the other way around. I've created this list, then I choose the database which location do have these sets of access points. Then you can find out of that you are here. I'm locating myself by doing so, there's no one else involved. When I'm building up that database, I know my current location.

I scan around the Wifi access points around me, and send that information to Google. During this process, I'm only using the Wifi access points, but the ICT department or people who own the Wifi are not aware that I'm doing this. With GDPR, that means I give my consent to Google to use my location.

If I am connected to eduroam, my device is connected to one of the access points. So if the ICT department know where the access point is, if they know the MAC address, and they have a map of all their access points, then they know this device is very near to the access point.

MAC address is a unique identifier for each device. If you know where the device is, then you know where I am.

Is the data anonymous? Yes, and no. If you can make a relationship between a MAC address with someone who is working in this building, you know that I work in this building, then you know that the MAC address is me.

I can only be connected to eduroam with my NETid. That contains my login details. My MAC address and my NETid are stored together. But the ICT department will never ever give that information.

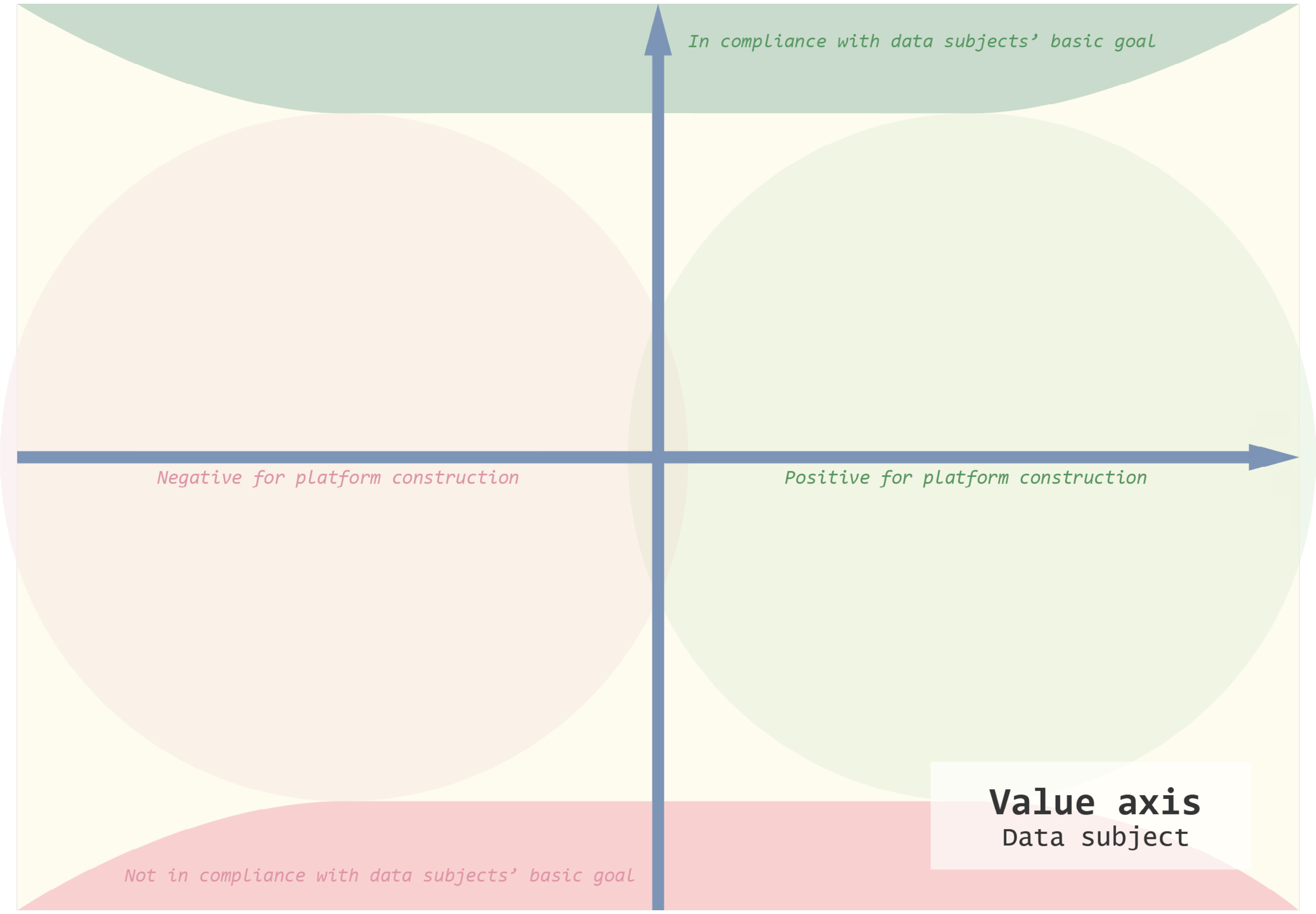
ICT will never ever give away MAC addresses. They will do some hashing, they will delete some data, before they give the data to the researchers. They only provide encrypted MAC address, so you can never ever refer back to the MAC addresses. So you only know that it's a specific device.

If I'm going to kill someone, and the police would like to know where have I been at this moment and time, then they will provide all the information to the police. So it depends on who want the data.

But still, if I detect a group of people inside this building, and I do know who are the employees over here, so I can still connect a group of anonymous people to them.

When your device is connected to the access point, a login entry is created. By default, the log isn't saved. But for the research project, the ICT turn it on to collect the data.

Appendix 5
Canvas for MVP 1&2


In compliance with data subjects’ basic goal
Negative for platform construction
Positive for platform construction
Not in compliance with data subjects’ basic goal
Value axis
Data subject

Value dilemma scenario

Value 1

Put a value card here

Platform construction

Stakeholder's basic goal

Conflicting with stakeholder B's basic goal?

□ Yes □ No

Conflicting with stakeholder C's basic goal?

□ Yes □ No

Value 2

Put a value card here

Platform construction

Stakeholder's basic goal

Conflicting with stakeholder B's basic goal?

□ Yes □ No

Conflicting with stakeholder C's basic goal?

□ Yes □ No

Inspiring quesions

1. What is the value conflict here?
2. Which stakeholder/value is more important in this senario?
3. How important is the value to each side?
4. ......

Inspiring quesions for potential features

Put a value card here

Who is the sub-value?

What is the most direct way to achieve this value?

How to involve them/other stakeholders to achieve this sub-value?

Is there any similar situation you could think about fulfilling the same value?

One feature to fulfill this value could be

Facts

MAC address and IP address are privacy, they are protectd by law.

Facts

From Wi-Fi access data, you can imply how many people are around an access point. You can imply the location of th people. You can see if the building is evacuated or not during an emergency.

Facts

It’s not difficult to find out a teacher’s MAC address. Because the timetable is usually open, so their MAC addresss will move at a certain time and location. So with extra information a certain persoan can be located.

Facts

If you want to study a group of people but you don’t know who they are, so you can’t ask each individual for consent.

Facts

There’s no standard procedure for researchers to get the data now. It’s just individual contact.

Facts

To log into eduroam, NetID is needed. That contains everyone’s identity information. But the ICT department will never ever give that information away.

Facts

When the device is connected to the access point, a login entry is created. By default, the log isn’t saved. But for the research projects, the ICT trun it on to collect the data.

Facts

A group of researchers were able to identify a particular person with his movement data in the campus, but only with extra information.

Facts

To implement GDPR costs efforts.

Facts

The data collected for ICT operation has a period of storage. Research is a legal ground to store data. The data used for research could be stored longer.

Data subject

Trustworthiness

Trust in the university

"[To share] the location data is okay for me because it's in the campus. I wouldn't want to share it if it's outside the campus."

Data subject

Trustworthiness

Trust in the law/policy

"GDPR makes me feel safe."

Data subject

Well-being

Benefit from service

"If it's for improving the Internet service, I can share my data though I don't want to. I really need the Internet here."

Data subject

Autonomy

Right to know

"If you tell me what you are going to do with my data, I will feel a bit more reliable."

Data subject

Goodwill

Contribution to good purpose

"I'm not okay to share my data as 'big data'--I'm more than willing to do so. I believe the school has a good intention, and it will be used for campus management."

Data subject

Well-being

Avoiding troubles

"As long as the data collection doesn't interfere with my real life, it doesn't matter."

Data subject

Security

Property safety

"My device information might reflect my financial situation and brand preference, it's very personal."

Data subject

Security

Personal safety

"Location is different, especially real-time location. It means others can find me using this information. It's scary."

Data subject

Trustworthiness

Distrust of the third party

"I'm actually not that worried that my information is being used inside the university. I just fear the information being leaked."

Data subject

Goodwill

Right to know

"I want the researchers to use my data to help others. But if you just tell me it's 'a research' with no more details, I won't share my information."

Data subject

Security

Avoiding being recognized

"Only anonymous is not different from real-name to me. Even though they don't know who it is, they still know it's a specific person. Everyone has a pattern. They can still find me if they want."

Data subject

Autonomy

Right to doubt

"Comparing to real-name, collecting my data anonymouly and analyze it as a specific person is even more weird. I would doubt its intention."

Data subject

Goodwill

Evaluation on the purpose

"My willingness to share my information is only based on relevance between my information and the purpose."

Data requester

Conformity

Conformity to regulations

“For research, you have other rulings on how to store the data, on how long you store the data.”

Data requester

Achievement

Concentration on the goal

“I don’t know exactly who initiated the projects. The teacher who organized the projects find the clients.”

Data requester

Achievement

Efficiency

“Wi-Fi access points are there to transmit data. It is available everywhere. You can use that already. You don’t have to do anything, and it’s free.”

Data requester

Achievement

Convenience

“The current procedure to get the data is quite informal. It’s like -’Let’s do it.’ -’Okay let’s collect the data then.’ ”

Data requester

Goodwill

Contribution to good purpose

“The main purpose of our project that uses Wi-Fi data is to optimize the usage of the facilities.”

Data requester

Well-being

Avoiding troubles

“Either you have to raise the issues with data providers, to tell them we are going to use your data, maybe there are lots of works with legal department over here because of lots of regulations, or you can also walk around it.”

Data requester

Security

Societal safety

“The data providers are not aware of the private issues. The researchers raise those issues.”

Data requester

Achievement

Authenticity of the data

“For research, I only want to know how many people are around here.”

Data controller

Achievement

Maintaining Internet service

“The ICT Department is collecting the data to provide Internet service. They moniter the number of users to provide enough accesss points.”

Data controller

Goodwill

Educational support

“There should be a shift, to shift more to ICT support for education and for research. That’s in the strategic policy of the board.”

Data controller

Achievement

Convenience

“The platform [for sharing data] will help the researchers not to interfere with ICT operation.”

Data controller

Achievement

Efficiency

“There’s no way I can get consent from everyone in the university. And filtering out you is pretty hard, because as soon as you get a new device, you have to tell me that is you.”

Data controller

Security

Societal safety

“The MAC address is encrypted when we give the data to the researchers, but technically you can recognize every device.”

Appendix 6
Cardset

Data subject

Trustworthiness

Trust in the university

"I only want to share my movement data inside the campus."

Is the data only being collected and processed inside the campus?

-

Is it only accessible from the people inside the campus?

-

Will it be pubilished publicly?

How to let the data subject know that the university is trustworthy?

Data subject

Trustworthiness

Trust in the law

"GDPR makes me feel safe."

Does the data collection, storage and usage comply with GDPR?

-

Does the data storage comply with the time limitation?

-

Is the data anonymised/pseudonymised properly?

How to let the data subject know that GDPR is implemented on the platform?

Data subject

Goodwill

Contribution to good purpose

"I'm willing to share my anonymous data because I believe the school has a good intention, and it will be used for campus management."

Does the research contribute to good purpose?

-

Does the research improve anything?

-

Does the research help anyone?

How to help the data subject to contribute to good purposes?

Data subject

Well-being

Avoiding troubles

"I'm willing to share my data if it doesn't interfere with my real life"

Does it bring any troubles to the data subject?

-

Does it influence the data subject's Internet experience?

-

Does it influence any campus management/service that may affect the real life?

How to help the data subjects avoid troubles?

Data subject

Well-being

Benefit from service

"If it's for improving the Internet service, I can share my data becaue I really need it."

Does the data subject benefit from any service by providing data?

-

Does their data directly improves the Internet maintainance?

-

Does their data contribute to other research that result in better campus service?

How to let the data subject know that they are benefiting from the service?

Data subject

Autonomy

Right to know

"I feel more reliable if you tell me what you are going to do with my data."

Does the data subject know for what kind of use their data is being collected?

-

Does the data subject know who use their data?

-

Does the data subject know what their data is being used for?

How to help the data subject know more about their data collection and usage?

Data subject

Security

Property safety

"My device information might reflect my financial situation and brand preference, I don't want to share it."

Does the data collection affect their property safety?

-

Does the data reflect their financial situation?

-

Does the data reflect their brand preference?

How to keep the data subject's financial situation private?

Data subject

Security

Personal safety

"Real-time location means others can find me using this information. It's scary."

Does the data collection affect their personal safety?

-

Is it possible for a data subject to be identified?

-

Is it possible that others can find the data subject?

How to keep the data subject secure while using the data?

Data subject

Trustworthiness

Distrust of the third party

“I’m not that worried about my idata being used inside the university. I fear the it being leaked.”

Is the data being processed to the third party?

-

Is it accessible from people outside the campus?

-

Is it lawful if the data is shared with the third party?

How to let the data subject know where does the data flow?

Data subject

Goodwill

Right to know

“I want the researchers to use my data to help others only if they tell me more details about the research.”

Does the data subject know if their data is being used for good will?

-

Does the data help the researchers help others?

-

Does the data subject know the purpose and result of the research?

How to let the data subject know that they are helping others by sharing data?

Data subject

Goodwill

Evaluation on the purpose

“I only want to share my data if I think it’s relevant to the purpose of usage.”

Can data subject evaluate the purpose of data usage?

-

Does the data subject know what is their data being used for?

-

Can data subject choose whether to share data based on the purpose of usage?

How to help the data subject know the purpose of their data usage?

Data subject

Security

Being anonymous

“Pseudonymisation is not different from real-name to me, because others can still find me with my pattern. Only being totally anonymous is secure.”

Is the data subject totally anonymised?

-

Is there a specific person’s behavior pattern?

-

Can they be identified with other information?

How to keep the data subject totally anonymous?

Data subject

Autonomy

Right to doubt

“Comparing to real-name data, collecting and pseusonymising it is even more weird. I would doubt its intention.”

Does the data subject has the right to doubt the data collection?

-

Can a data subject know more details about a reseach?

-

Can they stop sharing data to a research that they feel untrustworthy?

How to help the data subject have more control over their data when they doubt the intention of data usage?

Data requester

Achievement

Efficiency

“Wi-Fi access point is available everywhere. You can use that already, and it’s free.”

Does the data requester get the data efficiently?

-

How long does it take if they want an existing data set?

-

How long does it take if they want to collect a certain kind of data?

How to help the data requester get the data more efficiently?

Data requester

Achievement

Authenticity of the data

“I want the data to be authentic.”

Is all the data authentic and trustworthy?

-

Does the data requester know where does the data come from?

-

Does the data requester know if the data is 100% authentic?

How to help the data requester evaluate the authenticity of the data?

Data requester

Achievement

Convenience

“The current procedure to get the data is quite informal. You just talk to someone and you can start collecting data. ”

Is it convenient for data requester to get the data?

-

Is there any standard procedure to acquire data?

-

How many people they need to contact to get the data?

How to make it more convenient for data requesters to get the data?

Data requester

Security

Societal safety

“The data subjects are not aware of the private issues. It’s the researchers who raise those issues.”

Does the data requester help increase societal safety?

-

Do they raise data subject’s awareness of data privacy?

-

Can they stop those unlawful datasets being used?

How to help data requester increase people’s awareness about their privacy?

Data requester

Conformity

Conformity to regulations

“For research, you have other rulings on how to store the data, on how long you store the data.”

Does the data requester conform to the regulations well?

-

Is there any instructions about the ruling?

-

Is there any feedback to tell them if the conform to the regulations?

How to help the data requester better conform to the regulations?

Data requester

Achievement

Concentration on the goal

“The teacher who organized the projects find the clients and data, I don’t have to think about it.”

Can the data requester concentrate on the research?

-

Is there anyone else help them to get the data?

-

How long does it take for them to get the data?

How to help the data requester concentrate on their goals instead of taking much effort to get the data?

Data requester

Goodwill

Contribution to good purpose

“The main purpose of our project is to optimize the usage of the facilities.”

Does the data requester contribute to good purposes?

-

Do they get any feedback with their research result?

-

Are they informed if their result is getting implemented?

How to let data requester know that their research is contributing to good purpose?

Data requester

Well-being

Avoiding troubles

“We can tell the data subjects we are using their data and then do lots of works with legal department, or we can also walk around it because it’s grey area.”

Can data requester avoid troubles brought by the regulation?

-

Is there a legal way to walk around the problem?

-

How much procedure does it save if they avoid the problem?

Is there any ways to help data requester avoid troubles brought by the regulations lawfully?

Data controller

Achievement

Convenience

"The data platform will help the researchers not to interfere with ICT operation."

Does the platform bring data controller convenience?

-

How much time does it save if the researchers do not ask them directly for data?

-

How long does it take if they put the data into the platform?

How to help the data controller handle the data more conveniently?

Data controller

Achievement

Efficiency

"There's no way I can get consent from everyone in the university, because as soon as you get a new device, you have to give me your consent again."

Is the data controller handling data efficiently?

-

How long does it take to collect data that could be used for research?

-

How long does it take to prepare the datasets for data requesters?

How to help the data controller handle the data more efficiently?

Data controller

Achievement

Maintaining Internet service

"The ICT Department is collecting the data to provide Internet service. They moniter the number of users to provide enough accesss points."

Does the platform help the data controller maintaing the Internet?

-

Does it have more flexible data storage limitation that helps maintainance?

-

Does it save time from preparing data sets for data requesters?

How to help the data controller maintain the Internet better?

Data controller

Security

Societal safety

"The MAC address is encrypted when we give the data to the researchers."

Does the data controller help to increase societal safety

-

Does their data contains any personal information?

-

How difficult it is to identify a real person from their data set?

How to help the data controller handle the data to increase societal safety?

Data controller

Goodwill

Educational support

"There is going to be a shift for ICT, from operation to ICT support for education and research"

Is the data controller doing more educational support?

-

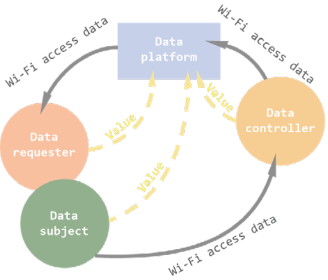
How many data requester does the platform help to get research support?

-

How research are supported with this platform?

How to help the data controller support more for education and research?

Context



How to incorporate values into data platform design?

Stakeholder

Data subject

The data subject are students, employees and visitors whose data is collected via Wi-Fi access points.

Stakeholder

Data controller

The data controller is the university ICT department that manages the collected data, and keep the data usage in compliance with GDPR.

Stakeholder

Data requester

The data requesters are researchers and students that request the data for research.

Autonomy

Can data subject vote for the research that they want to contribute?

Data subject

Autonomy

Can data subject follow up the projects that are relate to their everyday life?

Data subject

Security

Show the privacy protection method on the project page, so that the data subject know that their personal data is protected.

Data subject

Autonomy

Can data subject withdraw their data whenever they want?

Data subject

Goodwill

Can data subjects find the research result if it’s for good purpose?

Data subject

Trustworthiness

Can data subject find out where their data goes? (e.g. which faculty/outside the campus)

Data subject

Security

Can the platform categorize different data into different privacy level?

Data controller

Achievement

Is there a standard procedure for data requesters to request the data, that saves both side's time?

Data controller

Goodwill

How can data controller share data to more people (e.g. not only researchers, but also students) to support them?

Data controller

Security

Data requesters can only process personal data in data platform’s server.

Data controller

Achievement

Is there a standard procedure for data requesters to request the data, that saves both side's time?

Data controller

Goodwill

How can data controller share data to more people (e.g. not only researchers, but also students) to support them?

Data controller

Conformity

The data requester can only get the data when their research is GDPR compliant.

Data requester

Achievement

Show the data requester where does the data come from and how it was collected.

Data requester

Conformity

The data requester will get instructions on how to use/store/publish the data from the platform.

Data requester

Conformity

The data platform will help the data requesters to reach data stewards if they have questions.

Data requester

Achievement

Can the platform improve the collaboration between data requesters to help them achieve their goals?

Data requester

Conformity

Data requester will follow standard procedure to apply for the data, indicating for what kind of purpose they are going to use the data.

Data requester

Goodwill

Will the data requester get feedbacks of their research results?

Data requester

Security

How many people are responsible for one data set?

Data requester