AMIDST THE GOLDEN AGE OF PRIVACY

Gürses, Seda

2009

Gürses, Seda

Amidst the Golden Age of Privacy

> Transcription of the conference held on the occasion of the 12th edition of the Verbingingen / Jonctions festival in Brussels on 29 November 2009.

Conference: presentation Seda Gurses_Constant VZW

My main point today is that we should think of an alternative for data protection. In the rest of the talk, I am going to give reasons why I think we should think of an alternative to data protection as it stands today. The main underlying reason is that privacy, as a right, is focused on the individual and the rights of this individual. I'm going to propose that we should think of privacy as a social good. If we think about privacy as a social good, then maybe we also have to rethink data protection. Specifically I'm thinking of something like copy left for data protection, something that is not based on the concept of "personal data".

The title of the talk today is 'Amongst the golden age of privacy'. Never in its history has privacy been so voluminous and so productive. We have privacy conferences, we have privacy lawyers, we have privacy-speak, we have privacy films, we have privacy papers, legislation: it goes on and on. Today, I want to look at those side products and see what they are telling us about privacy. This is the grey matter that I would like to look at today. In order to do that, I'm going to start by showing you a couple of films.

Movie 1: a couple is sitting at a table in a coffeehouse, 'text balloon hearts' are shown above the people's heads with information of their profile: young, blond, long hair etc. As the couple comes closer, we see that an old woman sitting at the next table is manipulating the young man's profile such that his profile now states that he likes old women. The manipulation of the young man's profile disrupts the young woman as she's kissing the young man, who now moves to make out with the older woman.

Movie 2: In this movie we can see different ways of interrupting someone's privacy: when a person is in the toilet, when a person is calling on his/her cellphone, when a person is in his/her room. Movie ends with the message: Privacy is precious, handle with care.

The first two movies are from the Think Privacy Campaign to celebrate data protection day and to promote privacy amongst young citizens and can be found on YouTube.

Movie 3: The animation shows a little camera, the Google street-view camera, that is roaming the streets and taking pictures of certain areas. The camera then goes home to develop the pictures and to scan them for any privacy violations. If there is any privacy infringing information on the picture, the camera erases it before it continues with the other pictures.

Movie 4:Movie shows how a user can access 'Google Dashboard', where all personal data held by Google associated with the user provided with some controls. The objective is to provide users with more transparency and control.

Seda: 'It is no coincidence that these films are the way they are. The message of the first two films is very much concerned with fears upon the infringement of the heterosexual bedroom: if you protect your privacy, your bedroom, your sexual life and your sexuality will be protected as well.

How the current data collection and processing practices are going to disrupt the heterosexual bedroom is a topic in itself. Let’s leave that discussion for another time and remain focused on the “neutral” field of data.

We currently have privacy laws that companies that process our data have to comply by. These laws are called data protection laws. The main legislation to this purpose in the EU is the Data Protection Directive (95/46/EC). These laws are historically based on conceptions of the disconnected mainframes of the seventies and badly need updating to our current large and complex networks.

Data protection produces a vocabulary of its own. It talks about personal data, that is all data that is somehow directly or indirectly identifying an individual. Hence, personal data does not only consist of your name, address and birth-date: according to the data protection directive, any data that can be linked to an individual using reasonable means is rendered personal data. If some data refers to an individual, then that individual is a “data subject” of that piece of information. I’m introducing you to this peculiar legal language that we have to get used to, the latest because we are now all “data subjects”. Everyone in this room is at least a million times a data subject.

Data protection also mentions data controllers. These are the entities that data subjects interact with when they, or we, “give away” personal data. Data controllers are the ones who are supposed to provide privacy policies that indicate the purpose and means with which data is collected from the data subjects and how it is going to be processed. In return, data subjects are given the option to consent to the data collection and processing described in the policies. There are further terms in data protection, but the three I introduced, personal data, data subject and data controller, are sufficient for our current discussion.

These are the main building blocks of the legal language that is used to conceptualize what is popularly defined as “privacy as control”. This concept of privacy as control was also very present in all the films: they all depicted the importance of the ability of the individual to control their data, or disasters that may happen if this control is lost.

For a computer scientist with a security engineering background, this concept of control is misleading, because anything that is available on the Internet is basically uncontrollable and hence (pretty much disclosed to the) public. The concept of control over something on the Internet is meaningless. Therefore, if you want privacy, you have to hide it by default. You disclose only those things you want to make public. This is almost in complete opposition to data protection, which suggests that there is some middle ground. In order to do that, it provides natural persons with the legal tools to control the collection and processing of their data (through privacy policies and consent). It also provides them with some transparency as to how that data is actually being used through a mechanism called “subject access rights”. Subject access rights means the data subject can get in touch with the data controller, ask them about the personal data they hold, and request corrections or, if legitimate, their deletion.

In order to see how this works in practice, we recently studied privacy policies. We analyzed them to understand what they were saying and promising. We found that what they are doing is taking this data protection legislation, which is a very specific mode of protecting data based on an understanding of computers relic of the seventies. They are applying this legislation to things, like social networks, where, as Irma van der Ploeg says, the end of one machine and the beginning of another is not distinguishable. For example, if you look at the Facebook privacy policy, it’s very much about the ’you have control over your personal data" principle. It is however amended with further statements which in summary state: we collect another sizable set of data about you, but that does not count as personal data because you didn’t give it to us, we collected it elsewhere, hence this data is not about your privacy and is hence not under your control!

The reason that Facebook can add this amendment is partially because they are based in a different jurisdiction, where the definition of personal data is not as inclusive as in the EU. Another reason is because “anonymous data” is not protected by any legislation. Anonymous data is data that is not personally identifiable. Until very recently everyone thought that if you erased the name of a person and some basic data that uniquely referred to that individual, that data would be anonymous. Once data is anonymous, data protection states that it is free for exchange. This is pertinent to the two objectives of data protection directive: the first objective is to define some mechanisms to constrain data processing in order protect natural person's fundamental right to privacy, and the second to assure that the free flow of this data among member states can not be restricted or prohibited. Data protection is hence not only about protecting data, but assuring that it can flow freely across the borders of Europe and other countries that comply with data protection. The ability to make data anonymous is an essential element in creating free flows of data.

To conclude the study on privacy policies, the basic messages of the social networks to their users, as stated in their policies is as follows: (1)"we care for our users' privacy and our users can trust us" because we give them control over all the information that they volunteer. (2) We also collect all the traffic data of our users (who you communicated with and when), and data about our users from other websites/sources, but this is not personal data. The data that the users need to control is the one that they explicitly give us. (3) We also analyze the whole network (aggregate dataset), but this analysis will be based on anonymous data, so our users do not have to worry about this. (4) There are third parties and they are evil. Do not trust these third parties. Users should go and read their privacy policies but never trust them, unlike us.

We took the advice and went ahead and studied these third party privacy policies. We used a Firefox plug-in called 'Request Log' that listed the embedded pixels in each SNS website. We discovered a recursive situation. Each third party privacy policy states as usual "Trust us, we are good." Next, they state: "We work with third parties: they are not to be trusted like us. Read their privacy policies to find out what they are up to". So you go to the next level of third parties and you can actually draw a tree, it might even be a graph, of these third parties that claim that the evil is elsewhere, the privacy problem is always elsewhere and the user is in control.

Given this maze, whether the user has control is doubtful. However, what is constant is that the user is constantly given the responsibility for what happens to her data. The basic message to the user is: you have free choice, you decide what you are going to upload and then you control. Then come the exceptions: (1) if there is a security leakage (2) if your friends give away your data. (3) If you do not properly use the 200 privacy settings, which we change weekly, and this leads to privacy breaches, then this is your problem. Mind you, If I had 200 settings to control every day, I would also have a good sense of control, since I would be busy controlling the whole time. Hence, the policies relieve social networks of all responsibility for any unwanted disclosure of data by shifting that responsibility to the main actor of privacy as control, the user.

It is not that social networks are per se bad for privacy. On the contrary, it is the fact that social networks are "open" that makes it easy for communities to observe and organize collectively in response to unwanted governance of such social networks. I believe that such terrible privacy policies have actually been around for at least 20 years. But, I have never seen the Hotmail community get organized against Microsoft. In social networks, you do find that people start informing each other about things like changes to the Terms of Use, mobilizing "friends" into action.

There are so many protest groups in Facebook, that by now Facebook practices protest management. In the protests to the Terms of Use, Facebook co-opted the protests by suggesting that the users co-author these legal documents with them on their governance page. And because users were part of the process, Facebook could now say 'the authoring of the Terms of Use went through a democratic process'. There is really a lot to be said about what is happening under the name of democracy in Facebook, and I think it is worth watching. However, the basic line remains and only gets extended: you, the user, are not only responsible to control your data, but now you have to co-author and give legitimacy to the privacy policy as well: the document that puts all the responsibility on the shoulders of the user.

In the mean time, on the legal side, things also got more dramatic. The famous Lindquist case occurred, where a Swedish woman was convicted first by the Swedish courts and later by the

European Court of Justice, for disclosing personal data about her church congregation on her newly made personal website and hence breaching the Data Protection Directive, and introduced a new discussion into the realm of social networks. Mrs. Lindquist was doing a computer course. On her website she included pictures, names and telephone numbers of some of the people in her church. She was taken to court for breaching the data protection rights of her congregation: she processed data automatically without notifying the data protection authorities and did not ask for the consent of her church members. She was prosecuted and had to pay a fine. Ensuing discussions focus on a very decisive question: given that a typical user of a social network processes data about dozens of data subjects, hence such users all be seen also as data controllers. Now, if every user is a data controller, as soon as a user uploads information that has multiple data subjects (remember, we are all data subjects), she has to ask for consent from each and every data subject for the given purpose of the posting. Further, she has to provide them with the means to practice their subject access rights. It might be best for her to also have a data protection officer to make sure she is compliant at all times.

The Article 29 Data Protection Working Party, an entity expected to provide expert opinion on questions related to data protection, interpreted the Lindquist case and recommended that posting of personal data in social networks should fall under personal use. However, this is just a recommendation. At the end of the day, the judges have to decide, how they are going to interpret the Lindquist case for future cases. Waters are likely to get murkier when you have cases in which a Facebook user, maybe a political activist, maybe an advertiser, has 500 friends and stands in front of such a judge for data protection violations…

There are several points to be made here. First, there is a desire to solve everything legally, to use the privacy paranoia, the privacy worries and the actual concerns of people to legalize everyday life and as a consequence, to promote auto-control. Let me show you an example: this is a friend who got one of these famous quizzes on Facebook, where you have to answer questions and some unexpected and deep truth about life pops out of it. The information for the quiz includes her real name, her witness protection name, and it goes on, star wars name, her grandmother's name, etc. She gives this information. Within a few minutes she has comments from a friend: 'The answers to some of these questions are security questions that credit cards and passwords accounts use, may want to delete some of them'. Users have so internalized the privacy discourse that they start policing each other. Another friend responds: 'If I ran across something that is used for security, I use a different answer, I have multiple names when it comes to family names'.

This reminds us of the work of David Wills from the UK, who points out that bank security questions are prime examples of how the responsibilization of the individual citizens function. Governments and companies build electronic infrastructures, through which they get rid of intermediary personnel, rationalizing their work process. Users, customers, citizens are then burdened with the responsibilities of these rationalized workers: filing tax returns, booking flights, managing bank accounts, etc. All of this is done, usually with little care for system security and user interfaces. The culmination of which are peaked with security questions about odd things like "the maiden name of your grandmother". Next thing, there is a direct causality between maiden names of our foremothers and identity theft, supposedly the top privacy problem in many countries. Wills shows that this is not a privacy problem but actually a security problem on the side of the organizations that introduce such infrastructures, who are constantly using some personal data to give you access to their systems. All of a sudden, the customer or citizen is fashioned as the gatekeeper of that valuable data, and they are expected to do this for the sake of their privacy: a magnificent subversion of privacy concerns into user responsibility.

The conclusion I want to make here is that both data protection and definitions of privacy as control, actually focuses and responsibilizes the individual user and consumer: the weakest link in the data economy and related power structures.

Another problem with personal data is that when a number of people pool their data together, the concept of personal data may cut through the legal protection afforded to such common data. So all the disclosures to the public using, for example, creative commons licences, may also be subject to the data protection directive (if it includes personal data). This means that, if we want to be compliant, we have to learn to look at all data through the lens of personal data. Anyone can start making privacy claims with respect to public data. This could potentially re-introduce authorship into places where it is explicitly not desired. This is not happening yet, but the Lindquist case is going to open questions almost comparable to copyright, but for reasons of data protection and privacy, and these might be even more difficult to fight against than copyright itself. This parallel between copyright-think and data-protection think becomes especially evident, when engineers suggest using DRM to make sure personal data is processed in a compliant manner.

An alternative to data protection is to technically protect people's data. A good number of security engineers would dismiss data protection because it misses the rules of the Internet: anything you put on the Internet is impossible to control and is pretty much public. Hence, "preserving" privacy is equated to not disclosing any of your data to others. The only thing that similar between the technical approach and the data protection approach is its focus on the individual.

However, not only technically, but also socially and economically hiding your data is not trivial. Felix Stalder, for example, points out that in a networked world, what counts is not so much the data that is intrinsic to your person, but it's the fact that you are connected and that you can prove that you are connected. If we accept what Stalder says, the message of the security engineer to the individual user is double edged. The user has to make a decision: to hide her data and survive in isolation in a networked world, or give in and feel like a prototype of the "stupid user".

In order to demonstrate my point, I want to show you a film that explains how anonymous communication systems work (notice, this is different from the anonymous data mentioned earlier). Anonymous communications are one of the basic building blocks of privacy preserving technologies as proposed by security engineers.

Movie 5: In the nineties, privacy research started becoming popular amongst security engineers. Privacy was defined as 'the right to be left alone' and could be guaranteed in systems through data concealment. Specifically, security engineers were focusing on what they called anonymisation. Some researchers in Dresden, Germany, were specifically looking to anonymize cell phone infrastructures. Anonymisation meant that a third party could not infer by observing the cell phone infrastructure. Who were making phone calls? At what time? And from which location? In order to do this, researchers suggested adding encryption, dummy traffic and mixes to the usual cell infrastructures. Although these additions guaranteed significant anonymity, the researchers ran into an unexpected physical problem.

Two identical cell phones from the same manufacturer, coming out of the same assembly line, one after the other, had enough difference in their electromagnetic fields to be distinguishable. The electromagnetic fields could be used as signatures and utilized to trace the users. The researchers had not considered this environmental factor in their anonymity model. They were devastated. The Dresden researchers started collaborating with other researchers doing similar research in Scandinavia. They started discussing how they could achieve absolute anonymity. The Scandinavian researchers said 'let's imagine an anonymous city'. In this city, everyone should wear a box as soon as they leave their homes. These boxes should be as wide as the widest person on earth and as tall as the tallest person on earth. The boxes should be standardized so that they are indistinguishable. When the citizens walk, they should do so in the same manner and as slow as the slowest person on earth. This way they cannot be profiled according to the way they walk. If possible, they should leave their homes at selected intervals so that they cannot be profiled through the time in which they enter and leave their homes. Even better, dummy traffic should be introduced to the city, meaning two or more boxes should come out of each door. One containing the citizen, the others containing robots. When departing, the boxes should move in opposite directions so that is it difficult to distinguish boxes through their entrances and exits. Further, between two locations, different paths should be taken every time, so that the citizens cannot be profiled according to the paths they use frequently. In this anonymous city, the citizens have asked to give up some of their anonymity in order to be able to move in the city with their pets. As a result, we have added some anonymity boxes for pets. As they discussed further, and the inconveniences of the anonymous city became evident, researchers concluded that maybe this is not the way we want to live.

The point of anonymous communications is to make it impossible to distinguish who in a set is communicating with whom. Let us assume I do not know any of you in this room, If I would now close my eyes, and if one of you communicated with me, I would not be able to discern who it is. Based on your voice, I might guess your gender, infer where you are approximately in the room, etc. The more I collect such inferences, the more I collect some statistical information on who might have been the one that spoke to me. This is the kind of inference that security engineers working on anonymous communications try to minimize, so that when users are communicating on the Internet, communication partners cannot infer who you are, and other observers cannot find out who is communicating with whom. I want to take a step back and look at these anonymous communication systems critically.

Anonymous communication systems unlink the identity of the person from the traces they leave behind on the Internet. In a sense, they are distinguishing between three types of identifiers. One is the indexical identification, e.g., my name is Seda. Of course there are many Sedas in the world, but when you see me, you are likely to identify me as Seda. That is an indexical identifier. Another sort of identifier, is a pointer, e.g., I'm a Facebook user. This identifier points to me, now that you know that I'm a Facebook user. It is not my name but a pointer. Yet another type of identifier is the descriptive identifier. It again points to me but also describes me. The Facebook user is also descriptive. Descriptive identifiers are not really that distinct from pointers. Rather, there are some identifiers that are more descriptive and others that are just pointers. For statistical analyses what you need is descriptive identification. The indexical identifier, the name that is uniquely linked to me, does not necessarily have a descriptive element. The second identifier, a Facebook user, has a descriptive element. An anonymous communications system, hides the indexical identifier. It hides the fact that I'm Seda, but it actually keeps the rest of the information intact. What that means is that you can continue to do statistical analyses based on the traces that are left behind. This means you can continue to do behavioral profiling, which is actually what most of these companies say they are interested in. When we actually tell people they can protect their privacy by using anonymous communications, the only thing we are offering them is that possibly the company that they are communicating with, or the government, etc. can't indentify who they are, with respect to the profiles they have. But they still collect the profile information (without an indexical identifier, and in most cases, without knowing that different profile elements belong to the same person). The companies can still categorize and treat this information discriminately. Hence, anonymous communications are very useful for some communications, especially when you have an aggressive government and when you want to do something without being clearly identified, and you know you are not going to repeat the action enough times to be profiled. Then it is very useful. For such communications, it is imminent that we have these tools. However, in terms of the kind of general protection of privacy that many of us may be interested in, they don't actually offer any protection because the categories in these surveillance systems remain untouched.

Even worse, such surveillance and social sorting can continue to exist, even if some individuals decide not to give their information, as long as a critical mass continues to disclose their information. In such cases, those disclosing their data act as a proxy for those who prefer to conceal their information. Such dependencies require rethinking of the effectiveness of privacy preserving solutions in different contexts that focus on the individual.

In preparation of this talk, I wanted to find a way to step out of the data protection or security engineering discourses. Some authors, e.g., John McGrath, say that we have a lot of data bodies out there, we have a lot of traces that we leave behind or people have left for us, or we had to give in order to get access to a system etc. So we each have hundreds of data bodies that are out there. If you google your name, you will meet some of these data bodies that you didn't even know that you or any of your friends had left behind. So the question is, how should we relate to them? What kind of relationship should we have with them? Should we ignore them, should we love them, should we scream 'go away' or should we cry? What is the kind of emotion that we should develop? What is the relationship that we want to have with our data bodies that is outside of this legal and technical definition somehow? What is the relationship that we should have?

In order to explore these questions I asked my friends to send me objects that normally would identify them and I asked them to anonymize them. These have been on the table the last two days. I find it very interesting what people have sent. I'm going to go through these one by one to see what people are actually imagining when I ask them to think about anonymous data bodies. It is very revealing how different these reflections are form the legalese and the technical descriptions I summarized earlier.

One friend sent me an abstract of his paper. Statistically speaking, you can actually re-identify someone from written text. Actually, the first sentence would actually be enough, if the abstract is online, to re-identify him. Otherwise, you can identify him using his writing style. He felt it was anonymous. This friend sent this picture of a palm tree to me and she said 'I was very happy when I was at this spot where I was taking this picture and I think it is anonymous'. So this is her anonymous picture, it is a place where she feels very happy, it is a place where she identifies herself with, it is a different definition of identification in a sense and now it is anonymous, because we do not know who it is. Surely, the photo could be analyzed to identify the camera, and that could be used to link the photo to her, but this is none of her concern. Here is a painting of another friend. Anyone who knows her would recognize her right away, but in case you don't, her name is written here. These are the shoes of a friend. Turns out, this is her Facebook profile picture, which if anybody is friended with her, they will surely recognize this anonymous shoe fetishist. This is somebody in the room. This one was somebody who knows what securing engineering is. This one is from an artist in Istanbul. He made this drawing when he was 6 and had pneumonia and was in the hospital. He does not remember making it, but a friend visited him and my friend gave this picture to him. He thought this picture depicted a now anonymous memory. He said, "The one figure on the bed is me and I'm anonymous (even in memory)". I asked people to send me these through Facebook and I said I would put them up on Facebook, so you can see what everybody has sent. Facebook would not allow me to put this picture, since they are using some porn = naked skin recognition algorithm. And so even though these pictures are anonymous, they were too explicit for the Facebook filters and I could not upload them. It seems, Facebook has no problems with anonymity, but it certainly has many problems with sexuality. This is a passport picture. I will come back to that. And this one is from a friend who actually does material art. He uses camouflage material left from the GDR Army to do his art. This picture looks camouflaged.

From my generous sample, I conclude that people like to use forms of anonymization that come close to their personality: a data body that is distinct but related in a personal manner. I actually find it very interesting that these individual responses were each colored by own experiences, own desires, own imaginations of what it means to be anonymous and what it means to have privacy. There is also this postcard that I received. I turned it around and I couldn't find who it was from and I was going to almost rip it open to see if there was something hidden and then I remembered that I asked people to send me anonymous objects. I also received a letter that says: "if I were to send an image, I would have to deface it or render it unrecognizable. A gesture that is also against my own person if you believe in certain karmic energies…If our profiles are just data spaces, information spaces, if IP addresses are easily traced, if RFID tags accompany us through the objects we purchase and use, ID cards and passports now carriers of vital and important personal information, if our mobiles are basically first generation tracking devices, sound, voice, eye, fingerprint, breath become telltale devices for identification. Well, the blur is in the meeting of the immaterial and the material. Of wet ware, to soft ware to hard ware. How one is embedded in the other, and our relation to the object, and it's importance to our movements and dealing in our life. Yes, we all negotiate privacy and anonymity. Not the same things, to different degrees, depending on our education and life experiences about trust. I will leave it at that and hope this helps."

The last one, which I thought was really hard to digest, came from another friend who is on Facebook and he has actually tried to anonymize his profile, while remaining on Facebook. This awkward situation occurred because this person wrote an article in a book about homo-nationalism. Homo-nationalism is a recent formulation of a critique that is coming out of queer studies that is talking about the use of queer rights and women's rights in order to invoke some sort of legitimation for wars driven by the "western world" in certain other regions of the world. A couple of authors, one of whom sent me the letter, wrote about concrete practices of homonationalism. They were specifically criticizing the actions of an activist who goes to different countries to demonstrate the lack of gay rights almost always coupled with islamaphobic or ethnophobic statements. This person, who was the subject of their writings, called them and threatened to take the authors to court for writing this article. After this had happened, my friend wrote: ‘I would have liked to provide my Facebook profile, which I anonymized in order to keep myself safe-ish from this person. He has a huge Facebook presence, his fans are currently reporting people who stand for us to him, so that he can write them private messages. This mostly infects the inbred queer scene in Britain. But if I did that, if I gave you my Facebook profile, I wouldn’t be anonymous anymore’. So I exchanged some more mails and then he wrote back saying. ‘I’m so technophobic, so anonymizing is no easy task. You could use my pic and profile minus the name maybe. Even though I picked a nice name that means something to me. I still share a dozen or so of friends with a person who last week made a note in defense of this person with lots of abusive comments. So the anonymity reflects an ambivalent relationship to new media and Facebook sociality. Feel free to tell the whole story. Anonymizing us and the celebrity in your own words’.

This friend is so embedded in Facebook in his political activity that he did not want to leave Facebook. The problem became acute as his queer community split in two on the issue of homonationalism. Half of his friends were writing protective letters and notes while the other half were attacking and telltaling on them. It is very interesting to see how our lives are very much embedded in these systems. Anonymization is then not just about delinking traces, but it is about negotiating communities, negotiating spaces and networks etc. Neither the legal nor the technical experts can take care of these subtleties and we have to talk about these matters.

These are the points I wanted to raise today. To sum it up: the main point is that the concentration on the individual is not helping us. Data protection does it; the technologists do it, too. We need to find of way to have collective information and to disclose information without having to go back to counting each "personal data’ meticulously. I think such thinking can only be destructive while providing little protection. One last thing, I mentioned earlier that the Data Protection Directive states that if the data is anonymized, it is free of regulation. Recently, the research from computer science shows that in order to really anonymize data, you have to come close to noise, and that is pretty much useless to exchange. Now what is the problem with that? Many legal experts in Europe have understood that anonymity is close to impossible. In response, some experts suggest that data protection applies to anonymous data because it’s always possible to reidentify people by putting in reasonable effort. But, if we suggest that all anonymous data is reasonably likely to be identifiable, you need to have subject access rights for all personal data. If you have subject access rights, you need to know who the data originated from (who is the data subject). This means that data protection can be reinterpreted to mean that all transactions should always be uniquely identifiable. Without meaning to, such an interpretation can legally kill anonymity, while introducing a global surveillance system: an act one would not easily expect from privacy legislation.

Hence, it is now more than ever necessary that other communities start talking about how they can develop a protection of data that is not about individual protection and personal data.

So this is the talk, thank you.

****

Any ideas? ‘
Person 2 in the audience:’ I have, what is maybe a very naïve question, but I’m wondering about it from like the other side. Like why this data is useful to anyone? Like I guess there is money to be made of it, but like the information, the anonymous data, which isn’t anonymous, no I’m not sure how to phrase it…’

Seda: ‘No, I think you have a legitimate question…’

Person 2 in the audience: ' Like is the information that is profitable to someone, do I mind them knowing it. Or…like what is the relationship between what I don't want people to know and what their use for it is, or…cause a lot of the information that probably can be obtained about any of us, are things that wouldn't maybe bother us that people know.'

Seda: 'Yeah, okay, so I think what is important, I didn't talk about that, is the aggregation of this data. Generally, like the definition of surveillance that I take from David Philips says 'Surveillance is when you take data from individuals, and put them together, you have the whole population. And then you start doing analyses in order to recognize who fits some norms-you can define a norm once you have collected all the data- and who doesn't. And from there on you can start discriminating. This has become really normal practices in governments and in companies, even amongst us, we do it as well right, when we walk down the street. The people I have been reading and mostly from surveillance studies, says actually the modern state goes hand in hand with surveillance. So we cannot say that per se surveillance is a bad thing. So I think your question is a legitimate one. Now the problem is, we don't know how we are being surveyed, we don't know how we are being categorized, we don't know when we are being discriminated against, there is no feedback loop. It is very likely that there are certain groups that are constantly being discriminated against, because they are constantly falling to the wrong end of those population studies. And the question is what do we do. We cannot have…I don't think it is possible to say 'we should not allow them to categorize, because without categories I can't distinguish this chair from this table. And you know, we kind of need that. We are living in an economic system that is you know based on profit, whatever, maximization, rationalization. For this they do a lot of analyses. If we want to question that some more, I'm happy to talk about it. But I think at this point, we kind of have to accept that if you want to have these modern states conceptions that we live in, that you are going to have surveillance. Now the question is, what happens, it is kind of a wild west right now, anybody can do whatever they want and we don't know what they are doing so…this is a box that we are opening in a sense. And I think with individual data, I mean what google is doing with this dashboard , seeing my on-data brings nothing to me, I know it anyway, right. I really loved the performance earlier, if you kind of get this data right back to you, it doesn't mean anything, it's kind of this ridiculous repetitive thing and what is interesting is that when companies or those that are in power start taking those and saying this is your identity, and this is now who you are. This is how we profile and categorize you in this kind of profiling scheme. And they start defining who you are, instead of you who is kind of negotiating with them. And I think this is the problem. It comes back to identity in a sense.'

Person 3 in the audience: 'There is a very good example of that in HR companies because they harvest all this stuff. (Seda: 'Slow slow slow'.) Sorry, Human Resource companies harvest all the Facebook stuff and they profile you in their job specifications, so they use that against you. If then in the end your profile comes out, it doesn't match the job, you know what you said suggests it does, then you have a real problem. You shouldn't put anything on Facebook.

Seda: 'I think there are different prospectives on that, I think it's true that a lot of people are facing discrimination and I think we need to take that seriously. I think there are..There is Ronald Leens who we recently heard at the social network meeting and what he says is:' Shouldn't we also be questioning these employers who are using this data. And asking the question: 'is it okay to profile somebody through google before you meet them?' You know to ask them other questions in practice which are always brought down to 'the private individual didn't protect his or her data therefore for now she is going to be punished for that. Which I think we have to rethink in this digital era. Like what are we going to do if information leaks, like yesterday Matt F. was talking about. There is nothing we can do and why should I be individually paying the price for that and why shouldn't we as a society think about it. This is why I want to think of privacy as a social good and stop thinking about it as personal thing I have to defend in this big bad society.It's a very difficult role to put the individual in, I think.

We can also open the discussion to everyone, cause I am tired. And I think it is nicer if everyone responds to each other and I can sit there too and…'

Person 4 in the audience: ‘Just one question on privacy because I think privacy itself is a wrong term. If we just said, this document or whatever is private, it doesn’t mean anything, and the problem is, the fundamental problem is, the information wants to be free, the information wants to be distributed, it’s the purpose of informations. And I think the law itself is really bad because it’s focusing on the fact of the data itself and not on the user. Instead of they say, you have the use specification of the data but you don’t explicitly say what you will do with the data, what you are doing with the data, you don’t force companies to do so, so I think it is not to define it from a privacy, it is more to define illegitimate use of the data. But I think information wants to be free so you can’t change it.’

Seda: ‘I mean I think…these are the questions I want to ask. I want to think like…what if we had a copy left of privacy. Is it privacy? I don’t know even know what it is supposed to be called. I don’t like privacy because it constantly involves this individual, you know…’I’m in my walls and protected, my house is my castle, etc.’ Which I don’t think is true for a lot of women, but we will just take that…(laughs). And it also kind of has this autonomic subject, everybody is equal, there is a space in which they can think independently of society, these are really constructions that I have big problems with, and we are constantly migrating them into digital space and yes, the examples that are given are all about sexuality, they are all about showing body parts, they are all about, if you use drugs and if this comes out and it’s so weird that we are establishing very conservative lines, I mean…oh yes that’s the project, the Gaydar project. This is a project done by IMT students, they never published it, they gave an interview to a newspaper, very responsibly, where they said ‘we can look at your vicinity in a social network and figure out if you are gay or not.’ And I don’t know where to start with these guys, because first of all what they are saying is, it’s not even about you giving data, if we just look at your environment, we can infer who you are. So again, it’s a construction of identity from you know weird sets of information, right, and where is the diplomatics here. What makes you say that my network is my information source. And then, what is being gay? what does it mean to statistically infer something and say that is it now true? There are so many elements in here that need to be questioned. And I don’t know exactly where to start but I think these are the questions we have to ask, to think about, yeah I want that, I don’t want that…okay, one thing you can take out of the Gaydar thing is that not only should I not give information about myself, I should also try not to give information about others. So I should really keep quiet. So this becomes almost like a silencing example, which I really don’t like because most of the gay movement was about being public about your sexuality. And now I’m supposed to not say something because then you can infer that maybe my neighbor is also gay. It’s almost like a backlash on the gay movement right, if I take it as that example. So yes I want information to be free. Could I define something like: ‘I put data on the Internet, it might be identifiable, I don’t care, right’. Or ‘if there is profiling, it’s a commercially use of my data so therefore it’s illegal’. Something along those lines, that doesn’t go back to this individual personal privacy, atonomish subjects and you know like..I don’t know. This is just my imaginary.

It’s not on, the microphone, I think. An anonymous microphone is nice’.

Person 5 in the audience: ‘I was asking, can you explain a bit more about what you mean by copy left for private data or privacy, because I sort of intuitively understand I think what you’re aiming at but…’

Seda: ‘If I make a very big simplification as someone that knows very little about the copyright thing. The reason that you need copy left is because you cannot just say ’here is my text and I don’t want to copyright it, I want it to be freely available’. You can’t just put it online and it become freely available. Right, is this correct? You need to kind of go a step further, you need to use the law again in order for certain laws not to apply. So what I want, is a protection, that we define or that we think about defining, that doesn’t ever have to materialize, but it says ‘do not apply data protection to this’. It’s a legal category, but it says ‘do not apply whatever this consent to giving your data purpose, and I don’t know what else. I don’t know how to do this, right, it is a very difficult equation to solve. Because what they are saying right now is if I put data like ’Femke and I went to have coffee’ you can say that is personal data about me and you can say ‘I didn’t ask for you consent before I put it up on my social network’, whatever. Or if I put a picture of this event, it is possible that every one of you says ‘you didn’t ask for our consent, take that picture down’ Could be that’s already the case, I’m just saying that data protection can be another category to be used to pull that picture down and take me to court or whatever. Do you see what I’m trying to say.’

Person 5 in the audience: ‘Yes, but I also see that this of course something you see with copy left as well from a sort of legalization of communication. I’m not so sure whether…’

Seda: ‘I’m not either, I don’t know, It’s an idea, right. Like my point is how do I get away..I don’t know how to do it…but I’m just saying, let’s think about it. Think about a way to get out of this data protection matrix which is just too strong.’

Person 6 in the audience: ’Just a comment, I’m just thinking a lot. It is kind of interesting, I’m thinking in reference of a last talk where you mentioned actually you described good this kind of robot files which in a sense are this kind of ways of signaling to a search engine and not to do things like crawl(call?) or take data from a site and indeed that is a kind of mechanism to try to attack the problem of in a sense of the scale, the different kind I think of scales of a spider that it could sap all ??? of a site. Well I don’t know, there is a…just random thoughts. In some way it kind of connects, it’s almost like saying…you want to protect against certain data…END of Video