Identity processes

Why we put our most intimate details on internet and are still worried about our privacy

Winfried Tilanus, HAR2009

Summary

Many ICT-security problems are closely related to the to the notion of privacy. This, in turn, is closely related to our notion of identity. Very often researchers try to solve privacy problems without having a (solid) concept of identity. In this paper I will try to fill this gap.

In the social sciences there is a lot of work done around the concept of identity. A very powerful approach is that of 'cultural identity'. This approach says somebodies identity is not a property of somebody but a process of positioning inside a relation with somebody. So an identity is dynamic and always bound to a relation. Privacy can then be understood as the ability to influence your identity by controlling the information the other has about you. How you play this game largely depends on the expectations you have from the other and thus is different from relation to relation. Violating somebodies privacy is done by creating false expectations, for example false expectations of respect for a certain identity or a false expectation of secrecy.

To understand the privacy challenges the digitalization of our society poses, there are three types of relationships especially interesting. First there are relations like the ones of an ISP or an search-engine with their customers. Their customers expect them to be as invisible as possible, expect them to be just an enabler of communication with others. At the same time technology enables them more and more to take an active role, while commercial and legal demands might force them to do so. This double position makes them very vulnerable to public outrage and asks for careful operation. The second type of special relationships are the forced relations, for example because the partner is an legal authority or has an monopoly. From such organizations we expect care in the relation with us because we can't get a rid of the relation. This translates to demands like not using the information provided for other purposes and keeping secrecy. These organizations always had a lot of trust to loose, but the digitalization of society provides these organizations with an increasing amount of information they might violate. The last type of special relationship, is the panopticon-relation. Here an organization puts people under surveillance and incorporates a system of rewards and punishments in order to 'teach' them certain behavior. We accept to a certain level panopticons: think for example about schools and the enforcing of traffic traffic regulations. Before the digitalization of our society, the surveillance was the most expensive part of an panopticon. This is changing recently: the surveillance comes almost for free. Whether this results in a panopticon depends only on the presence of rewards and punishment. So it becomes more and more attractive for organizations to protect their interests by creating panopticons.

Introduction

There is a lot of confusion around the notion 'privacy'. Although we have an intuitive idea what privacy is about, when we try to define it, a lot of things become unclear: Where is privacy about? Is it for about information or about intrusion? (Austin) Why do we care a lot about privacy in one situation and not at all in an other? How comes most people care a lot about the privacy intrusion created by viruses and spam (Paine et. al.), but don't care at all about much more intrusive databases and surveillance systems. Why are we so irrational? And how exactly did privacy change in our networked and digital society.

Although a lot of research has been done on privacy, none of this research fully manages to answer these questions. Some research takes as starting point a descriptive approach to privacy. Burgoon et. al. for example describes four dimensions of privacy: physical privacy, interactional privacy, psychological privacy and informational privacy. Although such descriptions make clear what people might regard as privacy, the don't help us to understand what privacy is exactly about. Each of the four dimensions is so wide that this approach looses it analytical sharpness, it just doesn't help us understand what privacy is all about. A much sharper analysis comes from the juridical corner (Austin). This analysis can be of great help for lawmakers, for our purposes the analytical knife cuts away too much: privacy is reduced to "protection from public exposure". This approach to privacy can't help us to understand our seemingly irrational behavior when it comes to privacy. Other scholars (like Acquisti et. al.) call behavioural economics to the rescue. Strange enough he tries to understand our seemingly irrational behaviour, but doesn't scrutinize the concept of privacy itself.

I believe the research on, and the search for, privacy can be helped forward a by rethinking the concept of privacy. My starting-point is the vague intuition that privacy has something to do with 'identity'. I cherry-pick a concept of identity that might help us forward and then slowly move back to privacy, to how our seemingly irrational behaviour can be understood and finally to the level of the everyday digital practice and how the problems there can be understood.

Cultural identity

After the criticism of Foucault, the idea that humans have a fixed identity has become very problematic. Foucault has effectively shown, both in theory and with strong examples from practice, that we are determined by the relations we have and, most of all, the language we use in our relations, the 'discours'. Stuart Hall (1996) asks himself what is left of the concept of 'identity' after Foucaults criticism. Hall sees identity as two more or less opposing processes that are active at the same time: First of all the discursive processes Foucault described. In these processes differences between people are articulated. These differences are used to claim a different treatment between people. At the same time Hall sees a psycho-dynamic process of identification, thinking you are the same as somebody else. This makes identity a process that is always bound to a relation, a dynamic process of positioning. So identity is a process of positioning, it is bound to a relation and it always changes.

When looking at ICT-security, we should make a clear distinction between 'identity' and an 'identifier'. *Identity*, the positioning inside a relation, is a very complex exchange that can have interactions on many levels, think for example on the relations an employee has with and inside an organization. Such positioning might result, for example, in stating that somebody is

capable or trustworthy to do certain things. An *identifier* is a token handed out in the context of a relation. Examples are a passport, a drivers license, a SSN, a key, a credit-card, a username/password combination or a signed cryptographic key. These identifiers are handed out by one side of the relationship, when they feel the relationship is fit for it. Often that is at the moment a contract containing the rules is signed. Identifiers are used to give access to persons, places or assets, or to prove to third parties the existence of a certain relationship. When the relationship changes, the identifiers might be revoked. So your SSN for example, is the result of an identity-process and not your identity self.

Privacy & identity

In the context of identity-processes, *privacy* can be understood as:

> *the ability to influence the identity processes in a relationship by controlling the information the other party has about you*.

So privacy must always be seen in the context of how you position yourself in a relationship. When there is no positioning-process going on, e.g. when somebody is observing you and you never ever know it happened, there is no privacy aspect to it. According to this definition privacy is also limited to the control of information. Somebody who is standing too close to you has according to this definition on such not a privacy-dimension. But it can get a privacy-dimension if you loose control on information about you because the other standing too close to you (maybe the other smells you better or can observe you more closely). Controlling physical distance is just one of the many ways you might control information. Finally it is important to note that privacy, according to this definition, is not a binary entity, something you have or not have, but a scale, indicating to what level you are able to influence the identity processes by controlling information. Also giving a lot of information, but still being in control of the information results in a high level of privacy. Privacy is lost when the you can't control the information any more on which the identities are created.

To state it in another way: In each relationship you make new decisions on what information you want to be known to the other. This is an almost automatic process. This is a game where you play with the expectations you have from the other party and where you try to manipulate the way the other party sees you. By hiding, for example, that I have a past as long-haired, weed-growing hippie, I might try to avoid that a potential employer thinks I am not trustworthy. Or that drugs-enforcing agencies start digging in my past. But when I want to become intimate with some other hippies I might bring my past as weed-growing hippie to the foreground, hoping to gain credibility.

Whether I regard, for example, the digging in my past by the drugs-enforcing agency as a problem, depends on several factors. One is my expectation of their actions. Will they force a criminal identity upon me, or do I get an identity as 'irrelevant'? An other one is the question whether I will notice something from them at all. If they never let me know (in any way) they have investigated me, it wouldn't feel to me they have a relation with me. That would make them irrelevant to me. That also explains why people don't care about a lot of potential dangerous storages of data: they expect no problem with that organisation, or they even don't experience a relation at all.

We often make public 'opening positionings' to invite people to start in some kind of relationship. Walking around as long-haired hippie is an invitation to other people in the 'alternative circuit' to start a relationship with me, while at the same time it is signalling to other people not to position me as equal. This process is on the internet comparable to real live. The biggest difference is, that these 'opening positionings' might be visible to much more people, while the moral on the net puts much less limits on what is acceptable as positioning. So much more intimate details become visible to much more people.

Betraying privacy

So privacy helps you to control the identities that are created in relation with others. It is part of the positioning-game that is inherent to every relation and every communication. There are several ways you can 'betray' the other party in this positioning-game. The first way is to betray the the trust of your partner yourself. When I for example convince you that I won't judge you on your sexual orientation, and you confess to me that you are heterosexual, I might betray you by attacking you on being a conservative heterosexual conformist. Or more subtle: I might betray the relation my sexual partners have or had with me, by keeping an administration of the qualities and properties of each of them. In the context of digital privacy an example might be using visitor data to a website on mental health problems to build a database of ip-numbers and the likely disorder of the user of that ip-number.

An other way to 'betray' in this positioning-game, is to bring in a third party in the relationship that might have an other type of relationship with the other. Share your secret with me, and I will tell it through. Visit a website and a third party statistics system gets access to your movements on the site. Ask us for a vegetarian meal on board of the transatlantic flight and we will pass it trough to an agency that tries to determine whether you are a potential terrorist (and whether your access to a country should be denied).

It is interesting to have a look at 'identity-management' here. The term 'identity-management' suggest something even Orwell only would dream about (being able to manage the identity-processes would mean complete totalitarianism, far beyond even Orwells book '1984') . But 'identity management' usually means 'using one identifier in the context of several relationships'. A cryptographic solution where a trusted third party proves nothing more then that a user is the same as the user that created an account before has little privacy implications. That becomes different when the third party assures the user is the same user as an user in an other relationship, like a government issued digital token. When you are obliged to show such a token, you lose control over a bit of information about you. An other problem might arise when the token can be used to share information across relationships, like information-exchange systems as they are used in health-care or in a web-statistics system. In these situations the information provided in the context of one relationship gets out of my control and enters other relationships. I might have fairly different relationships with different health care professionals, and so have fairly different demands on what information I want to share. And unfortunately there is no general resolution to this: it depends from relation to relation what information is desired and what information is undesirable to be shared.

Challenges in a digital age

Carriers and interference

For our expectations it is very important whether we see an organization as passive channel that passes messages on or that creates a room to communicate with others, or as an active participant in the positioning game. This is a sliding scale. And although in reality no service is totally passive or neutral, we expect from a telecommunication provider or an internet access provider no interference (and thus confidentiality). We expect them to be on the passive side of the scale. The same is more or less true for a search engine: although we know the results might be subjective, we expect no interference on the individual level from the engine. One step further away from total non-interference on the scale are sites that enable us to communicate with others, like social networking sites. We know, and expect, that the freedom to use the service is only within certain limits, outside those limits we expect active interference. But still we regard them mainly as passive.

Nowadays, with digital communications and the ease of data storage, the organizations that are on the 'passive' side of the expectations, are in an extreme vulnerable position. Technically they are more and more able to become an active interferer in the relations they support, and legally they are more and more forced to do so. While at the same time they still see themselves as neutral institutions. The expectations from their users also lag behind: they still treat the service as a neutral enabler of communications. These organizations are in a serious risk of accidentally 'cheating' or being forced to 'cheat' in the identity games they are involved in. They can loose a lot of trust here.

Forced relations

People always had relations where they can't get a rid of. Many of the relations with authorities are an example of this: a lot of authorities will punish you if you try to break the relation you have with them. But also without punishment there are many organizations you are more or less forced to have a relation with. Not using water from your local water supplier for example, is at least very impractical. In many (democratic) societies, we believe that organizations that are engaged in such forced relationships, have an extra responsibility to act carefully.

The digitalization introduces new organizations that you can hardly get a rid of. But most of all, many organizations that already had a more or less forced relationship, are now presented with a wealth of information they can exploit. And it might be very tempting to do so. But often it is neglected that when we are in a forced relationships we expect care from the organization we have the forced relationship with. Much of the resistance against the new RFID payment system in the Dutch public transportation can be seen in this context: the participating companies have again and again demonstrated that they don't feel any responsibility to take extra care, although they have a forced relationship with their customers. At the same time the new payment system does provide them with an unprecedented amount of information on the movement of their customers. The digitalization makes for such organizations the responsibility a bigger burden.

Panopticons

In 1785 Jeremy Bentham invented a way to obtain power over the mind of prisoners, so they could be forced to adopt to social acceptable behaviour and be reintegrated in the society. His noble idea consisted of a round prison building with cages for the prisoners in the outer ring, with open bars facing towards the centre point of the ring. In the centre point a guard was positioned in a small booth with curtained windows to all sides. So the guard could observe the prisoners at any time, while the prisoners could not see if and when they where observed. The final step was punishing unacceptable behaviour. This system pushed the prisoners to acceptable behaviour: they could be caught and punished any time they went wrong. Foucault (1975) made an analysis of our modern society, using the original panopticon as metaphor: In many places in our society we are observed in a similar way an disciplined into certain behaviour. He concluded that the best way to find out if you are in a panopticon, is to check if there is a file on you. So for a panopticon there are four elements necessary:

1. Surveillance with filing on a individual level
2. Keeping uncertain when people are under surveillance
3. The aim to discipline people to a desired behaviour
4. A system of reward and punishment to condition people

When you are in a panopticon, your ability to influence the identity processes is strongly diminished. Not only is a panopticon designed to take away your control over the information about you, that information is deliberately used to control the identity-processes you are in. Privacy and panopticons are foes. But also note that we accept certain panopticons in our society. Schools are one example of accepted panopticons, our system for maintaining traffic regulations is an other one.

Since the invention of the panopticon 1785, the cost of creating and maintaining one has steadily dropped, while the panopticons themselves became more and more invisible. Until some decades ago the surveillance and filing where the most expensive part of maintaining an panopticon. Digitalization of communication and the advances in storage technology has dramatically changed this. Surveillance and filing on a individual level is nowadays in many cases an automatic by-product of the normal operations of organizations. Also the second element for a panopticon is nowadays omnipresent: we have no idea any more when we are under surveillance or not. So digitalization created an universe of potential 'panopticons'. The only things keeping them from becoming real panopticons is the lack of the aim to discipline and/or the lack of rewards and punishment.

So generally speaking we can say that the good news is: the internet has not yet created an world-wide panopticon. The bad news is that we are only two little steps away from one. When we decide to discipline people and create a system of reward and punishment for it, like the French three-strikes proposal, we create a panopticon.

Discussion

The proposed definition of privacy is a long-shot. It adds elements to the definition that are beyond the scope of the more regular definitions. It says privacy can only be understood within a relation. With the introduction of the identity processes in the definition, we also introduce the balances of power in the identity play into our thinking about privacy. Although that might seem scary or even contra-productive at first sight, it makes many processes much more understandable. This approach also gives a strong warning for researchers doing research on privacy: if you don't investigate privacy within a relation, the notion of privacy looses its meaning in your research. Whatever you investigate, it isn't privacy any more.

Despite it strengths, this view also has some weaknesses. First of all, there is the lack of empirical research. A lot of questions should be investigated, like: "Do we control information to influence identity processes?", "Does a loss of influence over the identity-processes by losing control about information about ourselves feel like a loss of privacy?", "Do we strategically make information about ourselves public when inviting others for new relationships?" and "Are expectations in the relationship a determinant for privacy-decisions?"

Beside the empirical foundation under this definition, a potential critique on this definition might come from Lisa Austin (2002). She opposes both to definitions of privacy that take control as central notion and to definitions that are centred around context and expectations. The problem with the first is, that loss of control doesn't per definition equal loss of privacy: only when the information that became out or control is also exposed to the public, she sees a privacy issue. Her problem with the second type of definition is the lack of normative power: It doesn't draw a clear line where privacy is violated or not.

Her first objection can be countered easily with two arguments: although the information might not be exposed to the public, according to my definition, there always has to be an other where the information is exposed to. And more important: not the loss of control over the information sec causes the violation, but the implications that has on the positioning inside the relation. The relation has to change because of it. But these arguments only make her second objection more applicable: my definition is strongly based on the context.

To counter her objection against contextual definitions, we need to step aside the argument: Austins project is an other project than mine: she tries to find a normative foundation to base privacy-laws on. Lack of normative power would be a major problem for her project. My definition doesn't try to provide such a normative power, on the contrary: I want to understand privacy, including the normative playing-field it contains. My approach helps to understand the normative dimension of something like the French three-strike law: that law says that internet users should be disciplined into certain 'correct' behaviour. It makes clear what norms the French government adheres and in what position it wants to see its civilians. My theory doesn't judge if that is right or wrong, and I don't want it to judge it.

Reading more

When asked about their privacy concerns, 16.1% of the respondents say: "Viruses" and 10.5% say "Spam". Source:

> Carina Paine, Ulf-Dietrich Reips, Stefan Stieger, Adam Joinson, Tom Buchanan; "Internet users' perceptions of 'privacy concerns' and 'privacy actions'" (2006); http://portal.acm.org/citation.cfm?id=1238548

Judee K. Burgoon has done several researches on privacy in real life. A nice peace of research on privacy in practice is:

> Judee K. Burgoon, Roxanne Parrott, Beth A. Le Poire, Douglas L., Kelley, Joseph B. Walther and Denise Perry; "Maintaining and Restoring Privacy through Communication in Different Types of Relationships" (1989); http://spr.sagepub.com/cgi/content/abstract/6/2/131

A very worthwhile article, digging deeper into different definitions of privacy is:

> Lisa Austin; "Privacy and the Question of Technology" (2002); http://www.springerlink.com/content/g1708p4118940782/

Some powerful work on understanding the privacy choices we make comes from Alessandro Acquisti. If you like a more economics orientated approach, then it is certainly worthwhile reading:

> Alessandro Acquisti and Jens Grossklags; "What Can Behavioral Economics Teach Us About Privacy?" (2006); http://www.heinz.cmu.edu/~acquisti/papers/Acquisti-Grossklags-Chapter-Etrics.pdf

All of the work of Foucault has been more or less centred around the notion of 'discours' and the various consequences of it. His most theoretical works on it are:

> Les mots et les choses. Une archéologie des sciences humaines (1966)

and:

> L'archéologie du savoir (1969)

He also wrote several studies on how it works in practice. First of all, his historical study about how we regard mental illness is noteworthy:

> Folie et déraison. Histoire de la folie à l'âge Classique (1961)

Very important for this article is his work on punishment and discipline. This work is mainly centred around the idea of the panopticon:

> Surveiller et punir. Naissance de la prison (1975)

My main source for my view on identity comes from the introduction by Stuart Hall, "Who needs 'Identity'?" in this bundle:

> Stuart Hall (Editor), Dr Paul du Gay (Editor); "Questions of Cultural Identity" (1996)

A very inspiring and often funny bundle on how identity processes work in practice, is:

> Antaki and Widdicombe; "Identities in Talk" (1998)

This paper is based on a presentation given at HAR2009, https://har2009.org/