Information sharing and privacy as a socio-technical phenomenon

Sotoudeh, Mahshid; Kamleitner, Bernadette

Veröffentlichungsversion / Published Version
Sonstiges / other

Empfohlene Zitierung / Suggested Citation:
Sotoudeh, M., & Kamleitner, B. (2019). Information sharing and privacy as a socio-technical phenomenon. *TATuP - Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis / Journal for Technology Assessment in Theory and Practice*, *28*(3), 68-71. https://doi.org/10.14512/tatup.28.3.68

INTERVIEW

Information sharing and privacy as a socio-technical phenomenon

Smart environments pose new challenges to information sharing and privacy. What does this mean for technology assessment?

The present proliferation of portable smart devices and stationary home assistant systems changes the ways in which people share information with each other. Such devices regularly have permission to switch on at any time and can collect a wide range of data in their environment. In consequence, the social challenge of personal data protection is growing and necessitates a better understanding of privacy as an interdependent phenomenon. Interview by Mahshid Sotoudeh (ITA-ÖAW).

TATuP: *Your recent research focuses on information sharing and privacy. What is the objective of this research?*

Bernadette Kamleitner: We show that privacy is a social issue, although people and policy makers seem to have little awareness of this fact. We all hold personal information about others. People are socially intertwined and bond with each other by sharing information. People's privacy thus not only depends on what people share about themselves, it also critically depends on what information others share about them. To capture this, we talk of privacy as being "interdependent." In an age of technology integration, this interdependence of data protection is becoming a major threat to privacy.

Could you illustrate this?

Let us imagine the following situation: Jane is waiting for a bus and wonders about tomorrow's weather. She is a chatty person, asks another passenger and gets the following response: "Sure I will tell you, but first give me the name and telephone number of your mother and maybe also a picture of her." Jane is furious and refuses. This is what usually happens in the offline world – people tend to respect and not give away others' personal information.

Let us now look at the digital world. Jane could consult a weather app, which might ask for access to her contact list. This includes details about Jane's mother and pretty much anyone else Jane knows. Yet, Jane might simply click "Install" and give away rather than protect information about others.

What are the possible consequences of data collection from individuals?

More and more devices are capable of tracking everything that happens around a person and people increasingly agree to everything being tracked or (inadvertently) do the tracking themselves. Often this includes their social ties. That this can have momentous consequences has become evident in the case of Cambridge Analytica. The company obtained the personal information of an estimated 87 million people from only 270.000 users who installed its app-based personality quiz. Presently, the issue of interdependent privacy constitutes a regulatory loophole even for the current best in class, the European Union General Data Protection Regulation.

How do you approach this phenomenon and what is the relation between privacy and property infringement?

There is not much literature on interdependent privacy infringements, perhaps because people intuitively respect each other's privacy in the offline world as Jane did in the bus shelter. Now that the problem arises in the online world, we lack the knowledge necessary to develop strategies that pre-empt or reduce interdependent privacy infringements.

Interestingly, there is a very pronounced parallel between privacy and property. The protection of both necessitates the cooperation of others and their respect for what is "ours". In contrast to privacy, the literature holds some insights into problems of interdependent property infringements. We thus looked at a vast range of cases of both interdependent property and privacy infringements to better understand why somebody gives away what is not his or hers to give.

How can we imagine this problem?

Essentially, the problem of interdependent infringements consists of a few key components. Let us go back to Jane and the weather app. Jane is what we call the "sharer". When she clicks "Install" for an app asking for her contact list, she not only gets the app's promised services but also says yes to its request to access all contacts of others as part of the download. All the contacts on her phone are what we call "the others", i. e., the parties getting infringed because they are connected to the sharer. The app provider that gets access to others' data via the backdoor of the sharer is the so-called recipient. By just clicking "Accept", Jane becomes a sharer of others' data to a recipient without those others even knowing about it.

https://doi.org/10.14512/tatup.28.3.68

Is the recipient the owner of the information?

Not actually. Legal data ownership would likely remain with the "other". Both sharer and recipient have access to information about the other, but whether or not the recipient has legitimate rights to this information largely depends on whether the sharer had the right to pass on that information.

So we have to ask: Why does a sharer pass on other people's information?

Based on our case analyses, we identified three hierarchical steps that a sharer needs to go through in order to NOT infringe what belongs to someone else. The first step in our 3R framework is *realizing* (R1). Jane might simply not realize that she is giving anything away when downloading the app. This can happen any time people do not check the permissions. People often fail at this step in the online world, but hardly ever do so in the offline world. Failure to realize also mostly happens for information, not for property.

The second step people need to go through is *recognizing* (R2). Sharers can only effectively protect others from infringement, if they recognize that their act of sharing concerns others. To protect what is not theirs, people need to recognize that others hold rights. In our example, Jane needs to recognize that although the data is on her phone, she might not have full rights to it.

The third and last step is *respect* for what belongs to others (R3). People need to be willing to respect the rights they recognize. Jane, for instance, not only needs to recognize that the data on her phone also concern others; she also needs to translate this into action and to ensure her contacts' consent before she shares their data.

How is "respect" relevant in your concept?

We refer to respect as the fair and lawful treatment of others. This means not risking to infringe what one recognizes as belonging to another. Of the three steps described, respect is the only one that has clear-cut moral implications. People only give away something they recognize as someone else's, if they feel that this is morally ok (such as "everyone does it, so it must be ok"), or if they knowingly put their self-interests first (such as "but I really wanted it"). In technology-mediated, digital settings, both self-interest and norms seem to facilitate disrespect for what belongs to others. This has already been well documented for digital goods, such as illegally copying movies or software. We also see it as a crucial issue when it comes to others' privacy.

What are the differences between privacy and property?

The primary difference between privacy and property lies in their targets. Privacy is the right to one's own information and personal space. Property is the right to one's own possessions. Possessions are something that we actively acquire and they are mostly tangible. Most property can be seen and touched, can only be held by one or few persons at a time (an exception are digital goods) and we usually know that there is someone who owns it.

In contrast, information is always intangible. People cannot see and feel it, and it is hard to trace its whereabouts. Information can also always be held by more than one person at a time, and it is nearly impossible to know how often it has been shared – that is why there are moral codes around personal secrets. Much personal information also does not become actively "acquired"; but simply arises as a side effect of our lives.

The nature of information makes it much easier to infringe privacy than property and we observe pronounced differences between privacy and property when it comes to our 3Rs. Infringements to privacy arise from failures at all the three stages whereas property infringements are mostly caused by a failure of *respect*.

How did you study the behavior of people?

We analyzed real-world instances of interdependent infringements, but also conducted experiments. In one of our most telling studies, we simulated an app download. Participants could choose to download a communication app after having to look at the permissions. Nonetheless, most participants significantly underestimated the amount of data they had just agreed to share. In one study, 96 % failed to realize what they had shared. Next, we showed them all the information they had given to help them realize the data transfer. To test for recognition we next asked who they thought had rights to these data. Most people said that their contacts were just their information, even if this included others' personal data. People appear to falsely belief that "If the information is on my device, it is mine." We next told people that this information also concerns others. Even after thus ensuring recognition of others' rights, about two thirds decided not to respect and protect others' data but to keep an app that they knew would access their friends' details.

Prof. Dr.
Bernadette Kamleitner

is head of the Institute for Marketing and Consumer Research and deputy head of the Department of Marketing at WU Vienna. Research topics include consumer psychology, ownership and digitalization.

What is the role of technology in interdependent infringements?

Technology has made it effortless to track and share information, even passively. After installing or even just purchasing devices, people automatically track and share data. For example, Facebook can track what consumers have done on over 8.4 million websites with the Facebook "like" button. However, people do not realize that this is happening. Due to the absence of any effort, people do not know what they are passing on, and sometimes they do not even want to know it. We can only respect others and our own rights, if we realize that our (passive) doings may affect these rights. If we do not realize that we are passing on information that does not belong to us, how is it possible not to infringe somebody else? We have become passive enablers of infringements.

Are we responsible, nonetheless?

We certainly are responsible if we knowingly disrespect others' data. When you see in the offline world that somebody is taking what is someone else's, you think of him or her as a thief and might try to intervene. Online, we see much less of this and people do not yet understand the dangers this might entail. For example, new possibilities on social media and the widespread illegal sharing of digital goods are at odds with moral offline codes.

Things are less clear when it comes to failures of realization and recognition. The technological possibilities and scope of data sharing defy most people's comprehension. What we now see is an exponentially growing potential for harm, but it is impossible to say what the exact consequences will eventually be and who will be held responsible.

To illustrate, let us imagine Emma and Mike meet at a party. They are close, and Emma confides to Mike that she has been diagnosed with leukemia. The party host has a smart speaker, such as Amazon Echo, who happens to be listening in. The party host becomes a collector and potential sharer of Emma's sensitive health details – an information he has not even been aware of collecting via his device. Whatever the actual consequences might be – technological advances combined with social interdependence make us vulnerable.

If we do not realize that we are passing on information that does not belong to us, we become passive enablers of infringements.

Do we need a new social learning process to deal with the new possibilities offered by social media, apps, etc.?

Yes! Technological advancements have happened so fast that we do not yet understand the full scope of their potentials and dangers. We have also had far too little time to develop social norms around it. Technology tends to be seen as lying outside of ethical or moral considerations, but it is not. Online there is a bit of an "anything goes" mentality. The social "stops" we are automatically adhering to offline are missing and self-interest and trivialization have free reign. It is high time that we start to synchronize online and offline social rules. Cambridge Analytica was a first lesson in that direction, but many more may be needed before this happens.

What does this mean for technology assessment?

Technology assessment (TA) could assess whether a technology is in line with established moral codes. It could also extend to ask which and how many actors can benefit from a technology or be (indirectly) harmed by it. TA can certainly help avoid that we end up in an uncontrollable social surveillance situation. Our social interdependence has been an enormous strength of our species. If we live that strength digitally with invisible but omnipresent tracking technologies, it can turn into a threat.

As a starting point, we need to make visible what information is tracked where and via whose device. Does the owner of the device realize and understand the scope of the information they are tracking? Does this information concern only them? If not, do they have the permission to share information about others? If the answer to any of these questions is no, then that device owner becomes a potential infringer of others' data. Our vision is a technology that automatically screens out everything that does not concern the owner of the device. Theoretically, this should be possible. Whether it is and will be done, is a different question.

Would it help make people aware of the information's value?

If information got a price tag, we might improve the realization of infringements, but this would come at a cost. The responsibility for passive information transfers would still rest with hopelessly overburdened individuals, and price tags could poison social interactions. If people realized that their contact lists etc. have monetary value, they might seek social connections for their monetary value. With devices that listen in, they might start to wonder how much a conversation, such as ours, is worth. If people can sell something, some will, and we all might think of each other as having different data price tags. This could trigger a hunt for the most valuable information about others. Putting a price on our social interactions might destroy them. En-

suring that there are some realms that are pretty much free from monetary considerations – where other values dominate – makes us humans.

Do you emphasize other solutions for enhancing privacy?

Yes! Ideally, we reduce the scope of the potential problem and set steps to avoid putting the blame on individuals. Technology can help remove the opportunity and temptation to (passively) collect and share information that concerns others.

Who is responsible for acting?

Because it is a social problem, it involves all of us and multiple stakeholders. We need to work on the legal and social rules, on the design of devices, and on additional technological solutions for data management systems. This means we need policy makers and regulators, industry self-regulation, innovators and entrepreneurs, consumer advocacy groups, and an informed public.

In our paper in the Journal of Public Policy & Marketing, we propose a toolbox comprising four classes of interventions suitable for different stakeholders. While the first three classes of interventions aim to improve current practices, we specifically advocate the fourth class, which proposes embracing radical alternative approaches.

What is radical about this class of actions?

Right now, privacy legislation mostly asks who has infringed and who is to blame. We use the word radical because the suggested interventions go away from the question of blame allocation. They focus on prevention of the problem and on moving control to potential victims of interdependent infringement. We suggest reinforcing efforts around privacy by design and by default, i. e., tracking less! In addition, we suggest delegating the responsibility for protecting one's own and others' data to privacy-enhancing technologies (PETs) or technology-assisted professionals.

How do privacy assistants and personal data managers work? What is their potential, and do you expect negative consequences?

These are technological or technologically assisted agents that learn the privacy preferences of their users over time, can then semi-automatically configure a range of settings, and make many privacy decisions on behalf of consumers who can thus maintain control of their privacy. From a regulation of personal data markets perspective, these would act as an extra monitoring mechanism and help redress the power imbalance in personal data markets.

We should start thinking of privacy as digital health and mandate a digital health insurance system on top of mandating a physical health insurance.

Nevertheless, if we put a price on privacy assistance, this might still end up tainting our social interactions. Another threat is that high levels of privacy may not be affordable for everyone. My personal vision is that we start thinking of privacy as digital health and that we mandate a digital health insurance system on top of mandating a physical health insurance. Having said that, data markets are international, so there are quite some challenges ahead.

Does the General Data Protection Regulation (GDPR) support radical interventions?

The GDPR does call for privacy by design and default. However, by and large, it focuses on individuals who provide their own data to an organization, and on what organizations – rather than consumers – do with data. There are loopholes when it comes to privacy infringements as acts of social interdependence.

Is self-regulation an issue in this concept to support privacy-friendly innovations? What else is needed?

Self-regulation in terms of what will be tracked, collected, and shared is an important solution. There are also excellent business opportunities in privacy-friendly innovations that, for example, screen out others' information. However, of course, if it is a business, it will bring its own challenges. Clearly, we need self-regulation and efforts by many stakeholders to ensure that our dear ones remain a source of strength rather than a threat to our privacy.