This is an invited paper for the symposium: "Who Owns Your Data" organized by Dennis Nguyen, Utrecht University of Applied Sciences, the University of Gothenburg and the Swedish Embassy. This is the authors' copy. The final version can be retrieved from: https://www.data-empowerment.nl/index.php/2021/04/26/grand-challenges-in-ethical-ux-a-case-for-privacy-coordination/

The correct APA reference for this paper is.Turnhout, K. van & Romero, N. (2021, April) Grand Challenges in Ethical UX. A case for Privacy Coordination. In Nguyen D. (ed.) Proceedings of the Who Owns Your Data? Symposium, Utrecht

Grand Challenges in Ethical UX. A case for Privacy Coordination

By Koen van Turnhout & Natalia Romero

Introduction

The datafication of society can best be characterized as a silent revolution. The rise of, subsequently, the web, social media, mobile computing, cloud computing and the internet of things has resulted in the availability of ever increasing amounts of usage data and a growing consciousness within companies that such data can be monetized. So, industry seized opportunities: business models changed, power relations shifted as new players 'disrupted' complete industries, and data scientists and programmers entered the workforce of many companies changing work practices and even the way companies define themselves.

Compared to such drastic infrastructural changes, the front-end of this societal change remained relatively inert. Costumers, users of sites, apps and smart products experienced smoother online interactions and a rise of novel applications and services – often for 'free' -, but this went gradual and was in many ways more of the same. Users never wondered what underlying data structures and practices were and to what extend they agreed with them.

Sure. They were asked to consent. Cookie notifications, privacy policies, and other forms of digital consent became an integral part of users' daily online diet. And users have clicked them away without much thought. This begs the question what the millions of user-approved clicks, collected daily, really mean? The façade of the consent button conceals that users were never in the position to make a 'choice' in the first place. They do not know what practices they are facilitating and they have no real alternatives. As such online privacy consent is simply a form of make-believe. Our society is living the collective myth of consensual data-practices.

Turn to design

Can we turn to design to bring about change in this situation? As the traditional mediator between technology and its users, designers ought to be in a position to address, what seems to be, a straightforward communication problem.

Some have argued for the contrary, even claiming that designers are part of the problem. Undoubtly bad design exists in the form of dark patterns

(Nodder, 2013; Gray 2018), so designers must address the question whether their practices are ethical (Monteiro, 2019).

But it would be a mistake to overstate the role of the designer in the creation of bad products. Design practitioners occupy a delicate position within companies and the economic tension fields surrounding those. As such, designers have a limited impact on strategic decision making. They also play an active role as ambassador for the user by balancing decisions in the interests of users, choosing for ethical practices and solutions, educating stakeholders about good design, and proposing alternative views of the future (Chivukula, 2020).

If we regard the myth of consensual data-practices as a design problem, we must not see it as a result of bad design but as a yet unsolved design "challenge". It ask us to turn to design research to help address it.

A grand challenge

Exempted from the practicalities of real world projects, design researchers can engage in self-critique, tackle design questions that transcend individual projects, and that are wider in scope and more fundamental in nature. They can explore innovative paths and nascent design spaces (Auger, 2016). One of the outcomes of design research can be what van Turnhout et. al. (2019) called "aspirational theory": theories that indicate what to strive for in design and how those ideals and values can be achieved.

If design researchers want to improve current data-practices, they must ask: what would be needed to put the users back in control of their data? Can we even imagine design solutions that allow users to share data with their service providers in ways that constitute both smooth user interaction and meaningful consent for specific data practices? Or can we go even further and give users agency and the ability challenge uses of data if they believe the inferences drawn from it are harmful or wrong (Mortier et al. 2014).

These are simple questions but wicked quests. We might, figuratively speaking, just as well try to put a man on the moon. In our view, giving users real control over their data is what Beck et al. (2017) call a big question or in our words a *grand challenge*. Luckily, it is not a new challenge and we are in a position to point to solution directions. For this we need the notion of privacy coordination.

Towards Privacy Coordination

If we are to change consent practices, we need to understand privacy in a different way. Most people think of privacy as an *information privacy* problem. Van de Garde (2009) defines it as 'the ability of the individual to control the terms under which his or her personal information is acquired and used by others'. The underlying metaphor is that of a transaction. The user gives a piece of information or data to another party under certain conditions (settled in a contract). In the act, ownership changes. As long as new owners comply to the conditions, they can use the information in any way they like.

This information-centred notion of privacy dates back to the 19th century, when recording equipment such as print and photography emerged. Print made it possible to present information about someone to a new audience after the event was over. It may be this possibility of second hand (mis)use which gives information privacy its ungraspable and ghostly feel. Debates on information privacy are often about situations that do not really happen, or at least not often enough to assess the risks reliably.

The difficulty of information privacy, from an interaction design perspective, is that it puts a high burden on the transaction moment. This is the only moment where the users can exhibit control over their data. They need to anticipate all future uses and limit those in very specific and formal terms. Luckily – note the irony here – this process is made easy by the companies, by drafting up the contract and limiting the burden for the user to sign the dotted line by pressing "ok".

The transaction model of privacy is so common that it will come to a surprise that it is an unnatural way of dealing with privacy. This has been pointed out by Irwin Altman in the 1970s. According to Altman, privacy is "an interpersonal boundary process by which a person or a group regulates interaction with others". Altman argues that, to understand privacy, we must see it as an ongoing coordination process between people rather than as an information transaction problem.

One example is communicating about availability status in the office. This is an ongoing multi-dimensional problem. At some moments you are more open to talk to others. It may also differ who wants to talk to you and for what reason. This requires coordination with your colleagues. You may signal availability by opening your office door when you're open to talk to colleagues, and closing it when you are not. You colleagues may barge in, despite the closed door. You may ask them to leave if they do so; and so on. It is a two-way process, it is ongoing – availability does not imply availability tomorrow -, and it is arranged through continuous lightweight communication. These characteristics create space for a much more course grained arrangement than a formal contract.

Although we do not advocate human-human communication as a model for human computer interaction in all cases, it is known that people treat computers essentially as social actors (Nass & Reeves,1998). This may explain why information privacy is understood so badly by users: they are applying the privacy coordination model they know from human-human communication.

The privacy paradox explained

One could argue that privacy isn't a large concern for users in the first place. Proponents of privacy sensitive solutions often face the counterargument that users give away so much data for free, that it makes no sense to try to come up with solutions that protect users' privacy in a better way. Indeed, there is well known discrepancy between what people say about their privacy needs and what they do online called the privacy paradox (Kokolakis, 2017). Users claim they care about privacy, but they do not exhibit behaviors that protect their privacy. One of the Facebook users in a study by Phelan et al. (2016) aptly summarized the general attitude: "It's creepy, but it doesn't bother me".

There are many explanations for the privacy paradox, and the verdict is out which one is the best, but taking a privacy coordination lens it is not hard to see why such a discrepancy between needs and behavior would exist. If human-human communication is the model people apply to privacy, privacy controls designed from an information privacy perspective, simply fail to meet their expectations.

People, for example, expect privacy control to be a continuous process. In human-human communication people privacy needs differ from situation to situation and if people felt they have been to open at a certain moment they can renegotiate the terms later on. Moreover, humans do so, typically, cooperatively, on the basis of direct feedback and concrete evidence of privacy violation and an equal 'power' to violate the others trust is case of a privacy breech.

This continuous, cooperative nature and direct feedback are absent online. There is simply no human equivalent to the Cambridge Analytical scandal where information that was intended for friends and family, was eavesdropped by a third party, to candidly feed highly targeted political advertisements, in the interest of a foreign superpower – all of this legitimized by 'formal consent', before users knew this was possible at all.

How could these users have known that their privacy would be violated and how could they have controlled it? Many data driven services utilize users data for purposes that are not in the users' awareness. No wonder they act carelessly. But we simply cannot blame the users who have been

disempowered by inapt privacy controls, that they are not behaving in a privacy sensitive way.

Designing privacy coordination controls.

The first to address the grand challenge of privacy coordination design was Natalia Romero (2009). She built on Altman's (1975) and Herbert Clark's (1996) common ground theories as well as on extensive fieldwork. These investigations culminated in a privacy grounding model and in design explorations implementing design coordination mechanisms. Based on her work and on considerations voiced earlier, in this essay we can point to several directions of privacy control.

1 *Dual control modes*. Most interfaces have a binary, single control character. Either you are or you aren't sharing information. But this doesn't have to be this way. Imagine an email to clients which allows potential senders to know the settings of your privacy filter and to breach it when it is important enough. It would allow for a much more gradual way of dealing with availability and it would enable interlocutors to decide to behave more appropriately. In everyday conversation we solve this type of coordination problems almost effortless, and non-verbally. The design difficulty for electronic privacy coordination support is to keep it as lightweight. It needs to be in the background, it needs to be easy to control and it needs to allow for ambiguity. Using the privacy grounding model, Romero did built tools which support lightweight communication of privacy needs.

2 *Continuous data ownership*. A somewhat deeper solution direction is to design tools in such a way that users have continuous control over their data. As a user I could share my email address to get a free gift, but after receiving an annoying newsletter I could revoke that access. One could argue that users already have the possibility to unsubscribe to newsletters, but this is a superficial solution. In our view, continuous data ownership would mean that users are able to remove all data-traces if they desire to and restore them if they feel this is desirable. Data traces only exist as long as users grant companies a licence. Such deep technical integration of privacy control would lead to data brokers such as IRMA, a Dutch, privacy by design initiative (Jacobs & Schraffenberger, 2020), which can be a decent solution in our view.

3 *Coupling of control and feedback.* A central quality of human-human privacy coordination is that the control of privacy is often directly coupled to specific breaches of privacy. If a co-worker shares something that was intended to be private information, it is normal to give them feedback at that point in time, causing them (and others present) to be more cautious in the future. This coupling of feedback and control is often lost online. An unwanted, targeted advertisement, is for most users unrelated to privacy

settings made earlier, elsewhere. But if users could give feedback on the personalized content they receive in such a way it would feed back into their privacy settings, a much more natural negotiation of privacy boundaries between the companies and users would emerge.

4 *Generic controls and adaptive defaults.* One reason privacy control online is such a hassle is that it has to be arranged from service to service. This is natural in the sense that in our social life what we want to share also depends on the specific social circles we want to share it with. Still we work with adaptive defaults. What we share is not negotiated in detail with everyone we come in contact with. We have a generic level of openness for a handful of circles, and a privacy breech, causes us to be less open for everyone. Online privacy could be arranged in the same way – at least when we decide to be less open. We could build tools grouping online services in default circles and arranging privacy settings for the group as a whole, and adapting it for the whole group when we feel reasons to change privacy.

Conclusion

In this paper we have set privacy coordination as a grand challenge for UX design. But it also has become clear that it is not only a problem of UX design. Regulations should be adapted to give users more rights and developers more possibilities to give the users privacy controls that they can understand and use.

References

Auger, J. (2016). Project Grounded Response. In. Joost, G., Bredies, K., Christensen, M., Conradi, F., & Unteidig, A. (Eds.). (2016). Design as Research: Positions, Arguments, Perspectives. Birkhäuser. P044.

Beck, J., & Stolterman, E. (2017, June). Reviewing the big questions literature; or, should HCI have big questions?. In *Proceedings of the 2017 Conference on Designing Interactive Systems* (pp. 969-981).

Chivukula, S. S., Watkins, C. R., Manocha, R., Chen, J., & Gray, C. M. (2020, April). Dimensions of UX Practice that Shape Ethical Awareness. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1-13).

Clark, Herbert H. *Using language*. Cambridge University Press, 1996.

Garde Perik, E. M. van de (2009). *Ambient intelligence & personalization: people's perspectives on information privacy.* PhD Thesis. Eindhoven University of Technology.

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018, April). The dark (patterns) side of UX design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (pp. 1-14).

Jacobs, B., & Schraffenberger, H. (2020). Friction for Privacy. Why privacy by design needs user experience design. In Wekke, K. van der (ed.), European Cyber Security Perspectives 2020, pp. 12-1

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security*, *64*, 122-134.

Monteiro, M. (2019). *Ruined by design: How designers destroyed the world, and what we can do to fix it*. Mule Design.

Mortier, R., Haddadi, H., Henderson, T., McAuley, D., & Crowcroft, J. (2014). Human-data interaction: The human face of the data-driven society. *Available at SSRN 2508051*.

Nodder, C. (2013). *Evil by design: Interaction design to lead us into temptation*. John Wiley & Sons.

Phelan, C., Lampe, C., & Resnick, P. (2016, May). It's creepy, but it doesn't bother me. In *Proceedings of the 2016 CHI conference on human factors in computing systems* (pp. 5240-5251).

Reeves, B., & Nass, C. I. (1996). *The media equation: How people treat computers, television, and new media like real people and places*. Cambridge university press.

Romero Herera, N. A. (2008). *Coordination of interpersonal privacy in mediated communication.* PhD Thesis. Eindhoven University of Technology.

Turnhout, K. van, Jacobs, M., Losse, M., van der Geest, T., & Bakker, R. (2019). A Practical Take on Theory in HCI. *White Paper.* HAN University of Applied Sciences. Available from: (http://bit.ly/TheoryHCI)