4 SUMMIT VIENNA 2015 IS IS

Extended Abstract

Lessening the Burden of Individualized Responsibility in the Socio-technical World

Judith Simon [12,*], and Irina Shklovski [2]

[1] University of Vienna, Universitaetsstr. 7, AT-1010 Vienna
[2] IT University of Copenhagen, Rued Langgaards Vej 7, DK-2300 Copenhagen S.

E-Mails: jusi@itu.dk; irsh@itu.dk;

* Author to whom correspondence should be addressed; Tel.: +45-72185325

Accepted:

Distributed Epistemic Responsibility

Contemporary practices of knowing take place in increasingly complex, distributed and dynamic socio-technical environments. However, despite a recognition of the socialness of epistemic practices in social epistemology, and a recognition of the role of technology and instruments for knowledge creation in philosophy of science and technology, many epistemological concepts are still astonishingly individualistic. One concept we deem central to understand contemporary knowledge practices is epistemic responsibility. Understood individualistically, epistemic responsibility refers to the responsibilities of knowers in giving and accepting reasons, of assessing the credibility of information providers and sources (Origgi 2008), or of being a good informant (Craig 1990). Clearly, the ability to act responsible in knowing has changed profoundly due to various technologies of information, computation, communication we use in our daily quests for knowledge and we need a notion of distributed epistemic responsibility to account for these changes (Simon 2014). In particular, we argue that individualized accounts of epistemic responsibility not only fail to capture the nature of contemporary knowledge practices, but also that they are potentially harmful by ignoring issues of power and fairness within knowing. One aspect often considered profoundly important for the assumption and attribution of responsibility is the availability of information. Only if I have information about the credibility of information sources, only if I can offer information to back up my knowledge claims, am I able to act responsibly. However, the availability of information while being necessary, is not sufficient for acting responsible in knowing.

Terms of Service: Providing Information, Shedding Responsibility?

Consider for example the case of personal information management in dynamic socio-technical environments. Knowers are held responsible for revealing information online, ensuring their passwords are secure and making decisions about whether to allow or deny applications access to information such as their physical location on various mobile devices. In most cases, knowers are presented with information about the services or devices they use via Terms of Service (in the event of a purchasing or signing up for a free service such as an email address) or an End User License Agreement (in the event of obtaining an application for use). Where the Terms of Service (ToS) are a set of rules the user must follow in order to be allowed to use the service, the End User License Agreement (EULA) is a license given to the user by the provider for the right to use the application. These types of documents detail the activities the user and the provider are allowed to engage in and typically specify terms of engagement with user data (what kind of data can be exchanged, how it might be used by either party, what kinds of rights and obligations each party has). For example, by accepting the EULA in the process of installing smartphone applications users give permission to access a range of their use data and to utilize it for a variety of purposes (Kelley, P., Cranor, L. & Sadeh, N. 2013). Considerable efforts have been made in designing for better and easier presentation of permissions and rules users actually agree to in this process and by producing various supportive tools to assist with knowledgeable decision-making. Yet research repeatedly shows that smartphone users do not have a good idea of what they are agreeing to when installing applications (Good et al., 2005; Felt et al., 2012;). They may not read EULAs at all or, if they do, they may have a hard time understanding the technical language (Kelley et al., 2012). Given that users must make an ongoing, practically never-ending series of decisions when installing, updating, sharing, setting permissions for the services and applications they use it is no wonder they exhibit fatigue and eventually a kind of learned helplessness (Shklovski et al, 2014; Andrejevic, 2014).

Accordingly the availability of information about the way personal data is dealt with does not necessarily or even predominantly result in responsible action. Users are drowned in information either impossible or impractical to process and moreover there often are no real opt-out possibilities beyond not using specific services at all. So it seems that information provision can sometimes not only be insufficient for responsible action (on the side of the user), it can actually be a form of delegation or shedding responsibility (on the side of the service provider). Thus, similarly to the introduction of informed consent in the realm of medicine, the availability of detailed information regarding the terms of service can be seen as a form of responsibility shedding rather than as a form of user/client empowerment.

How to support a fair distribution of responsibility

Given this situation, what can be done to enable and support epistemically responsible behavior and to distribute the burden of responsibility fairly? To our mind, three approaches must be considered and ideally combined:

1. Intermediaries designing tools and services to support individual responsible action.
2. Hard law solutions for issues such as data protection.
3. Technology development for de-centralized security solutions

Intermediaries: One way of managing the weight and pressure of personal responsibility for navigating the thickets of information about permissions and data practices is through the creation of intermediaries that can simplify and support individual responsible action. One example of such an effort is a recent launch of PrivacyGrade.org - a project run by a group of researchers at Carnegie Mellon University - intended to provide an easy guide for ANDROID users about the data practices of the applications they may want to install. The website lists applications and gives them a letter grade - from A for very privacy sensitive to D not privacy sensitive. The website contains links and information on how the evaluations of these apps are made, what algorithms and models are used and how privacy is conceptualized (Lin et al., 2012). The transparency of the evaluation is designed to engender user trust as a way to negotiate just how much information should knowers need to assess in order to make informed and responsible decisions. One problem with services such as PrivacyGrade.org is that they still endorse a rather individualistic understanding of epistemic responsibility. While the team of PrivacyGrade.org is certainly supporting users to assess the privacy implications of their choices, the action to inform themselves and act accordingly is left entirely on the side of the users. It is their responsibility to use the services, to inform themselves and to make informed choices, there is no *default* protecting them. In order to more fairly distribute the burden of responsibility over different actors, we need other types of governance alongside these efforts.

Hard Law: Responsibility is not only a duty of users, but also of service providers. One way to ensure that service providers meet their responsibilities towards the users is through hard law. Cases of particular interest for epistemic responsibility are data protection regulations as well as privacy laws. Only if there is a basic protection of private data can users be reasonably expected to act responsibly themselves. Given the pervasiveness of data leakage it is no wonder that users refuse to read EULAs and continue to give access to their data despite expressed discomfort in doing so. This perceived futility of self-protection may lead to fatalistic acceptance of constant data leakage as the inevitable norm, resulting in learned helplessness. After all, the "inability to protect one's private zones is a sign of absolute helplessness in defending one's basic interests" (Margalit 1998, p. 120).

Technology Design: In the time of fast-paced technology development, hard law often can not keep up with the rate of technological advance, thus technical tools such as decentralized secure data platforms that can enforce how personal data is accessed and used are necessary. Recent advances in security and secure systems research and development of secure data and usage control layers for mobile technologies offers solutions at the level of technical infrastructure. This is another way that responsibility for personal data management can be shifted from resting entirely on the user to application developers and service providers as they must contend with the inherent structural limitations of such secure systems (Danezis et al., 2012; Anciaux, Bonnet, Bouganim & Pucheral, 2014).

Conclusions

These are different types of governance to increase responsible action in knowing - distributing responsibility over different agents - industry and government alongside users. While each one of these alternatives is currently vigorously pursued, this research is mostly done in isolation. We argue that to achieve fairly distributed epistemic responsibility these lines of research must interact in order to produce complementary solutions.

Acknowledgments

Judith Simon wishes to acknowledge the financial support of the Austrian Funding Agency (P-23770).

References

1. Anciaux, N., Bonnet, P., Bouganim, L., & Pucheral, P. (2014). Trusted Cells: Ensuring Privacy for the Citizens of Smart Cities. *ERCIM News, 2014*(98).
2. Andrejevic, M. (2014). Big Data, Big Questions| The Big Data Divide. *International Journal of Communication, 8*, 17.
3. Craig, E. (1990). *Knowledge and the State of Nature: An Essay in Conceptual Synthesis*; Claredon Press: Oxford, UK.
4. George Danezis, Markulf Kohlweiss, Benjamin Livshits, Alfredo Rial. (2012). Private Client-Side Profiling with Random Forests and Hidden Markov Models. *Privacy Enhancing Technologies*. Vigo Spain.
5. Felt, A., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012). Android Permissions: User Attention, Comprehension & Behavior. *SOUPS '12* NY: ACM
6. Good, N., Dhamija, R., Grossklags, J., Thaw, D., Aronowitz, S., Mulligan, D., et al. (2005). Stopping spyware at the gate: a user study of privacy, notice and spyware. *SOUPS '05* (pp. 43-52). NY: ACM
7. Kelley, P., Consolvo, S., Cranor, L., Jung, J., Sadeh, N., & Wetherall, D. (2012). A conundrum of permissions: installing applications on an android smartphone. In *Proceedings of FCDS12* (pp. 68-79). Berlin: Springer-Verlag, Heidelberg
8. Kelley, P., Cranor, F., & Sadeh, N. (2013). Privacy as part of the app decision-making process. In *Proceedings of CHI 13* (pp. 3393-3402). NY: ACM
9. Lin, J., Sadeh, N., Amini, S., Lindqvist, J., Hong, J., & Zhang, J. (2012). Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. *UbiComp '12* (pp. 501-510). NY: ACM
10. Margalit, A. (1998) *The Decent Society.* Cambridge, MA: Harvard University Press
11. Origgi, G. (2008). Trust, authority and epistemic responsibility. *Theoria*, 61, (pp. 35–44).
12. Shklovski, I., Mainwaring, S., Skúladóttir, H., & Borgthorsson, H. (2014). Leakiness and Creepiness in App Space: User Perceptions of Privacy and Mobile App Use. In *Proceedings of the 2014 ACM international conference on Human Factors in Computing (CHI 2014)*, Toronto, Canada: ACM.

13. Simon, J. (2014). Distributed Epistemic Responsibility in a Hyperconnected Era. In *The Onlife Manifesto – Being Human in a Hyperconnected Era*; Springer: Dordrecht, Netherlands, (pp. 145-159).

© 2015 by the authors; licensee MDPI and ISIS. This abstract is distributed under the terms and conditions of the Creative Commons Attribution license.