The role of privacy impact assessments in shaping privacy-protective technical solutions

Haleh Asgarinia

Introduction

The widespread use of apps in response to COVID-19 raises concerns about privacy. Understanding the extent to which technology affects privacy and data protection is a core aspect of the Privacy Impact Assessment (PIA). PIA is a methodology for assessing the impacts on privacy of a technology that involves the processing of personal information, and taking remedial actions to avoid or minimize any negative impacts. PIA involves two basic steps: first, identifying and evaluating risks to privacy and second, considering ways to avoid or mitigate those risks. However, for implementation a third step, implementing those mitigation measures, is then required. This final step should ideally occur through privacy-by-design (PbD).

The purpose of the current study is to determine *the role of PIA in shaping privacy-protective technical solutions,* in this case the role of PIA in shaping PbD. I argue that the analysis of the role depends on how to approach PIA in that different approaches evaluate apps differently, which in turn, various measures and tools will be identified to reduce privacy threats.

Privacy Impact Assessments

1. The Contextual Approach

The contextual approach to PIA highlights the social dimensions of privacy and describes privacy as a normative conception, instead of a neutral one. In this approach, context is interpreted as social spheres, as constituents of differentiated social space. Instead of considering values that privacy is presumed to support, this approach focuses on privacy itself.

An assessment in terms of interests and values involves three layers.

1. In the first layer, PIA should study how apps affect the interest of key affected parties, including users and those who were in contact with them: information collected by apps is about them; physicians or health centres: information are sent by them; and health authorities: information is transmitted to them. In this layer, the benefits the parties enjoy, the costs and risks they suffer should be analysed.
2. In the second layer, PIA should study whether different parties involved in the context are ethically treated by assessing parameters such as unfair discrimination, equal treatment, and reputation.
3. In the third layer, the impact of apps on contextual values, ends, and purposes, public health, in this case, should be assessed.

The CI framework holds that a right to privacy is a right to appropriate flows of personal information, which varies from context to context. Appropriateness of a particular flow of information is determined by analysing whether context-relative informational norms are respected. Overall, CI insists that appropriate information flows serve the interests of different parties in the context, and context-specific values. Therefore, if information flows generated by apps negatively affect each layer, they are flagged as violating information norms - privacy.

2. Measures to Preserve Privacy

The second step of PIA is to determine the role of impact analysis on providing measures to preserve privacy. Here, legal decision-makers play an important role. They need to define terms and conditions under which information transfers from party to party in the given context, to ensure that the flows are fair and just. It follows that policymakers contribute greatly to the impact analysis of app in the second layer of PIA.

3. PbD: Effective Tools to Minimize and Mitigate Privacy Risks

In addition to legal decision-makers, app developers also need to play a role in preserving privacy, at least in the first and third layers of PIA. In the first layer, privacy should be protected by designing user control mechanisms, which allow users to know the purposes for which their information is collected. Key parties have the responsibility to prevent information from falling into the wrong hands. It is their professional responsibility to deal properly with the flow of information within the realm of their own activities. Thus, a shared responsibility approach can also be used in developing apps.

Furthermore, in the third layer of PIA, app developers need to adopt value-sensitive design approaches, particularly integrating context-specific values into app design. Developers and engineers should be aware of how their design creates or changes values for users, context, and society. In this way, they must consider values as design choices.

Summary

Our approach is important in determining the role of PIA in shaping measures to protect privacy. The contextual approach to PIA evaluates the impacts of apps in three different layers. Accordingly, different measures need to be developed to reduce privacy risks and improve privacy safeguards in each layer. Consequently, performing PIA within the CI framework highlights the relevance of user control mechanisms, shared responsibility approach to design, and context-specific value design in privacy-friendly apps.

Reference:

Mobile applications in support of contact tracing for COVID-19- A guidance for EU EEA Member States. (2020, June 10). Retrieve from https://www.ecdc.europa.eu/en/publications-data/covid-19-mobile-applications-support-contact-tracing

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review* (79), pp. 119-157.

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford, CA: Stanford University Press.

Nissenbaum, H. (2015). Respect for context as a benchmark for privacy online: What it is and isn't. In B. Roessler & D. Mokrosinska (Eds.), *Social dimensions of privacy: Interdisciplinary perspectives* (pp. 278–302). Cambridge: Cambridge University Press.

Raab, C. D. and Wright, D. (2012). Surveillance: Extending the Limits of Privacy Impact Assessment, pp. 363-83 In Wright, D., and De Hert, P. (Eds.), *Privacy Impact Assessment: Law, Governance and Technology*, Series no. 6. Dordrecht: Springer.

Strauss, S. (2017). *Privacy Analysis- Privacy Impact Assessment, pp. 143-156 in Sven Ove Hansson (eds.), The Ethics of Technology.* London; New York: Philosophy, Technology and Society.

Van de Poel, I. (2009). Values in engineering design. In Meijers, A. (ed), *Philosophy of Technology and Engineering Sciences: Handbook of the Philosophy of Science,* (pp. 973-1006). Elsevier.

Whitelaw, S., Mamas, M. A., Topol, E., van Spall, H. G. C. (2020). Applications of digital technology in COVID-19 pandemic planning and response. *Lancet Digital Health* (2): 435-440.

Wright, D., and De Hert, P. (2012). Introduction to Privacy Impact Assessment, PP. 2-23 in Wright, D., and De Hert, P. (eds.), *Privacy Impact Assessment*, Law, Governance and Technology Series No. 6, Dordrecht: Springer.