How is Positive-Sum Privacy Feasible?

Christoph Bier[1], Pascal Birnstill[1], Erik Krempel[1], Hauke Vagts[1,2] and Jürgen Beyerer[1,2]

[1] Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB, Karlsruhe, Germany
[2] Vision and Fusion Laboratory, Karlsruhe Institute of Technology, Germany
{christoph.bier|pascal.birnstill|erik.krempel|hauke.vagts|juergen.beyerer}@iosb.fraunhofer.de

Abstract. This work discusses Ann Cavoukian's fourth *Privacy by Design (PbD)* principle, which is known as *Full Functionality – Positive-Sum, not Zero-Sum*. The authors argue that this principle regulating trade-offs between privacy and functionality is questionable from a theoretic as well as from an operational point of view. A more consistent and pragmatic definition of *positive-sum privacy* is proposed and demonstrated using an example scenario in the context of video surveillance.

1 Introduction

Ann Cavoukian's seven principles of *Privacy by Design (PbD)* are as well recognized as appreciated in the privacy community. Nevertheless, according to their rather abstract nature, they are often hard to apply in practice. In particular the fourth PbD principle of *Full Functionality – Positive-Sum, not Zero-Sum* seems overly dogmatic. Hence, Section 2 illuminates this principle and its consequences in detail. Given these insights, Section 3 proposes a revised definition of *Positive-Sum Privacy*. Section 4 applies this new notion of *Positive-Sum Privacy* to a video surveillance example, before concluding in Section 5.

Related Work

Besides the discussed PbD Principles by Ann Cavoukian [1], who introduced the term in the early 1990s, Langheinrich [2] was one of the first researchers who focussed on the application of a PbD framework. His principles for system design are based on the Fair Information Practices Principles (FIP) by the OECD [3]. Guerses et al. [4] criticise the missing distinctiveness of the PbD principles. They propose to start from data avoidance as the best and first step towards PbD.

2 Discussion

Ann Cavoukian's fourth PbD principle *Full Functionality – Positive-Sum, not Zero-Sum* [1] addresses the compatibility of privacy and functionality.

> "Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum 'win-win' manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretence of false dichotomies, such as privacy vs. security, demonstrating that it is possible, and far more desirable, to have both."

Figure 1 illustrates the three different concepts from game theory needed for understanding Cavoukian's definition as well as the revised version in Section 3. Depending on a starting point (dots in Figure 1), functionality F and privacy P can evolve. Changes are denoted with ΔP and ΔF respectively.

- zero-sum: A concept in the field of game theory in which the sum of the outcomes is equal to zero (cf. Figure 1a), i.e., a positive ΔP results in a negative ΔF with the same quantity and vice versa.
- positive-sum: A concept in the field of game theory in which the sum of the outcomes is greater zero (cf. Figure 1b), i.e., either ΔP or ΔF can be negative, but the sum is positive.
- win-win: A special case of a positive-sum game where it is necessary that every participant has a outcome greater zero, i.e., privacy and functionality increases (cf. Figure 1c).

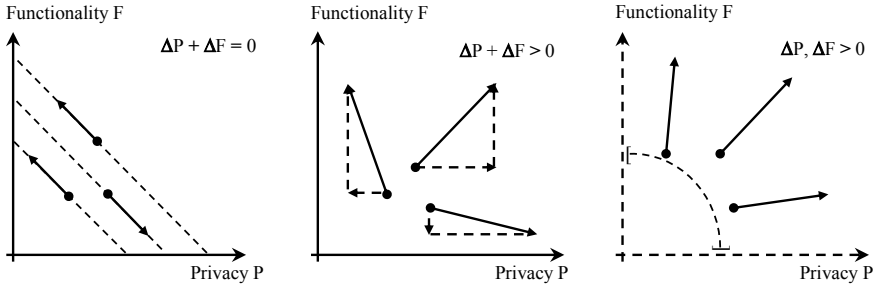
In other words, fulfilling this principle of PbD requires that a given system's functionality must only be extended if at the same time the systems privacy-awareness is improved. This requirement inhibits any kind of pragmatic trade-offs, i.e. neither tolerating a minor cut of functionality for significantly improved privacy nor sacrificing a bit of privacy for undoubtedly beneficial functionality is possible.

The principle is also inconsistent from a theoretical point of view. Starting with a situation of full privacy and zero functionality, adding functionality that requires personal information necessarily reduces privacy. Generally speaking, there have to be trade-offs between functionality and privacy in some cases.

In order to assess whether a new design results in a win-win, positive-sum or zero-sum situation, the degrees of privacy and functionality have to be measured. For this, privacy as well as functionality requirements have to be prioritized and weighed against each other. After determining to which fraction the requirements are actually fulfilled by a given design, the weighted sums over the fractions of privacy and functionality fulfillment can be calculated. From an operational point of view, however, weighting of requirements is a controversial issue and developing a method for objectively resolving conflicting requirements is an open research question.

3 Positive-Sum Privacy

As discussed in 2, a more pragmatic regulation for trade-offs between functionality and privacy during a concrete design process requires a new definition of *Positive-Sum Privacy*. A design process does not necessarily start from scratch,



(a) Zero-Sum (b) Positive-Sum (c) Win-Win

Fig. 1. Comparing zero-sum, positive-sum and win-win

i.e., privacy invasive features are often created by adding new functionality to an existing system. Thus, the new definition also has to be applicable as a guideline for the evolution of a system.

Definition 1 (Positive-Sum Privacy). *Positive-Sum Privacy consists of a starting point (cf. Figure 1), an evolutionary step and an assessment of the method:*

- *Starting point of a comparative evaluation is an outdated predecessor with less than full functionality and less than full privacy, both greater than zero.*
- *In an evolutionary step, a trade-off between privacy and functionality is acceptable if and only if it results in a positive-sum of functionality and privacy.*
- *The positive-sum has to be clear and not based on biased evaluation methods. If there is reasonable doubt, Positive-Sum Privacy is not fulfilled.*

It must be stressed that PbD cannot assure that a system is not privacy invasive. When adhering to all seven principles of PbD, however, one can come up with a design that is as little privacy invasive as possible given the purpose of the system. As a consequence, particularly for a system whose purpose is intirinsically privacy invasive, it makes perfect sense to establish a PbD compliant design process. This insight will be illustrated in the subsequent section.

4 Positive-Sum Privacy in Intelligent Video Surveillance

As starting point for this example assume an airport being monitored using a conventional video surveillance system, which is supposed to be replaced for efficiency reasons. The purpose of the video surveillance system is to observe critical infrastructures of the airport, i.e., regions of the airport that must not be accessed by unauthorized persons. The system is also used for manual tracking of intruders, thus its cameras do already cover the airport to a great extent. The security personnel is faced by a large number of live video screens.

Video surveillance is often criticized as an unselective measure putting people under general suspicion, i.e., a very high privacy impact is inherent to video surveillance. Nevertheless, modernizing video surveillance due to efficiency needs is an opportunity for carrying out a PbD compliant redesign.

The new system shall enable security personnel to observe critical regions more efficiently, i.e., intrusions have to be detected autonomously, so that an operator can concentrate on handling incidents. In the default setting the system performs rather noninvasive intrusion detection. Person detector algorithms are only running on specific cameras that cover critical regions and the cameras' video streams are not shown to the operator. Thus, *no* personal data is stored. If and only if an intruder is detected, the system is put into *alert mode*, which enables logging of the operator's interactions and tracking of the intruder.

By this means, system functionality is separated into a less privacy-invasive default operational mode, i.e., intrusion detection for critical regions, and a highly invasive alert mode, i.e., tracking or locating of intruders. This design is compliant to *Positive-Sum Privacy* as in total the system is less privacy invasive and only in highly selective situations trades privacy for valuable functionality.

5 Conclusion

The new definition of *Positive-Sum Privacy* allows for pragmatic trade-offs between privacy and functionality as often required in practice. The field of intelligent video surveillance illustrates the benefit of such trade-offs. An entirely rephrased and complemented definition of PbD as a set of explicit requirements of a design meta-process is ongoing work.

Acknowledgment: This work was partially funded by Fraunhofer Gesellschaft Internal Programs, Attract 692166, the KASTEL project by the Federal Ministry of Education and Research, BMBF 01BY1172 and the SURVEILLE project in the 7th Framework Programme by the European Commision (Project reference: 284725). The views expressed are those of the authors alone and not intended to reflect those of the Commision.

References

1. Cavoukian, A.: Privacy by Design - The 7 Foundational Principles (2011)
2. Langheinrich, M.: Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. In Abowd, G.D., Brumitt, B., Shafer, S., eds.: Proceedings of the 3rd International Conference on Ubiquitous Computing (UbiComp 2001). LNCS, Atlanta, GA, Springer (2001) 273–291
3. OECD: Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Organisation for Economic Cooperation and Development (1980)
4. Gürses, S., Troncoso, C., Diaz, C.: Engineering Privacy by Design. In: Proceedings of the 4th International Conference on Computers, Privacy & Data Protection, Brüssel (August 2011)