Privacy Mediation Cards

Imprint

Privacy Mediation Cards

Media Informatics and Multimedia Systems

University of Oldenburg
Escherweg 2
D-26121 Oldenburg
Germany

https://hci.uni-oldenburg.de/

Edited by: **Susanne Boll**
https://susanneboll.de/

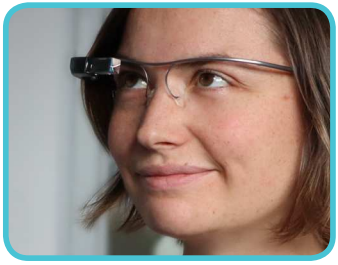
Written and designed by: **Marion Koelle**
https://marionkoelle.de/

ISBN: 978-3-00-061565-8

Privacy Mediation Cards

Why Privacy Mediation?

On the one hand, using personal, body-worn cameras can be great fun. On the other hand, these “always-on” cameras are not well accepted in social situations, as they may cause discomfort and social tension, and even intrude others‘ privacy. Ensuring privacy in the context of body-worn cameras means that bystanders should have the right and ability to choose when, where, and by whom they are recorded. Various technologies can facilitate this process by mediating between camera user and bystanders. We call this Privacy Mediation.



Body-worn cameras can come in various shapes and sizes: attached to clothing and accessoires, or integrated in glasses.

Privacy Mediation Cards

This card deck

This card deck – the **Privacy Mediation Cards** – introduces technologies and principles that can be put together to create privacy mediating procedures for various kinds of body-worn devices with an integrated camera.
This card deck **helps teams of designers and developers to broaden their thinking**, and **develop solutions** for socially adequate usage of body-worn cameras that go beyond making a binary decision for either banning or allowing body-worn cameras. On the long run this shall aid to smooth the adoption of body-worn camera technologies and make it more considerate to all stakeholders involved.

Acknowledgements

The development of the Privacy Mediation Cards has been supported by the BMBF project ChaRiSma under grant number 16|1665. Numerous reseach colleagues contributed ideas and criticisms to the design process without which the card deck could not have been completed. Those are:

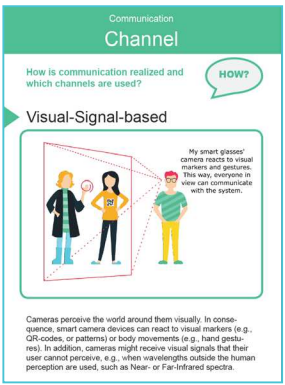
Andrii Matviienko
Luna Nicolaus
Sebastian Weiß
Shadan Sadeghian Borjojeni
Tim Stratmann
Torben Wallbaum
Uwe Grünefeld
Vanessa Cobus
Wilko Heuten

Privacy Mediation Cards

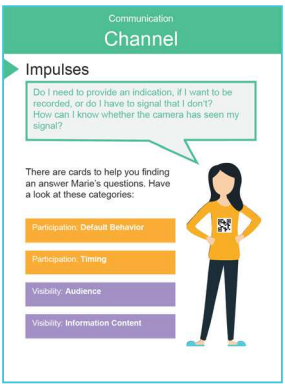
Where and how to start?

The 34 Privacy Mediation Cards are structured in 6 categories: **Communication**, **Visibility**, **Participation**, **Enforcement**, **Implementation**, and **Responsibility**. There is no predefined order or hierarchy.

Each card has two sides:



Concept



Impulses

One **concept side**, presenting a technology, principle or concept that answers to a design question.

One **impulses side**, presenting potential problems or questions, and pointing to card categories with potential answers.

Privacy Mediation Cards

Where and how to start?

The card deck is intended as a tool to gain an overview of privacy-mediating procedures, and a mutual basis for discussions. Two exemplary ways to start are:

1. **Explorative**: start from any one of the impulses cards, and explore the linked categories.
2. **Problem-oriented**: start from a problem you encountered with your product, prototype or design. Explore the solution space by spreading all cards (e.g., on a table). Then, pick one concept and start exploring alternatives (e.g., from the same category) or extensions.

Keep cards with concepts you like, discard those you don‘t. In the end, use the cards you kept to design one or more solutions to be further discussed.

Feedback

The range of technical opportunities for Privacy Mediation is coninously evolving; and so should this card deck. Your feedback can contribute to this process.
We would love to get into a dialogue with you about your experience with our Privacy Mediation Cards and learn how they might have helped you to come up with solutions.

privacymediationcards@uol.de

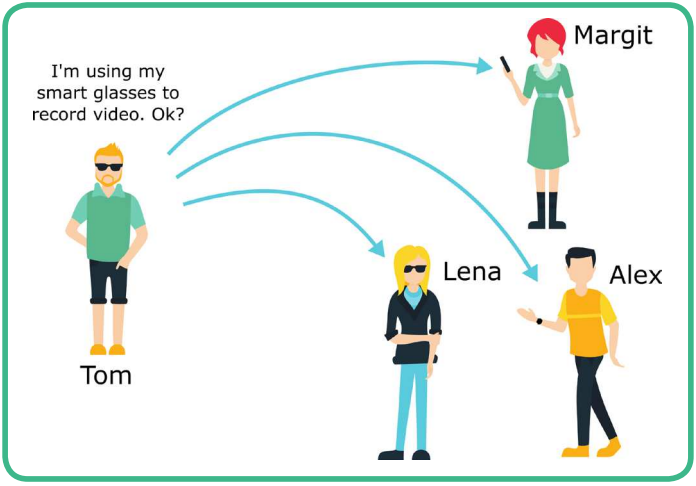
https://privacymediationcards.uol.de

Initiative

Who should take the initiative to initiate privacy mediation?

WHO?

The user



A privacy mediating procedure can be designed in a way where the user of the camera device or the camera device itself (here: Tom and his smart glasses) proactively initiates privacy mediation. Then, a verbal request or a computer-generated message is transmitted from the camera device to other participants (here: Margit, Lena, Alex). Recipients could ignore the message, acknowledge it or react to it (e.g., by sending a response).

Communication

Initiative

Impulses

What happens if someome‘s response to my smart glasses‘ inquiry is that they do not want to be recorded? Am I responsible for protecting their privacy?

There are cards to help you finding an answer to Tom’s questions. Have a look at these categories:

Enforcement: **Kind of Enforcement**

Enforcement: **Obligations**

Implementation: **Compliance**

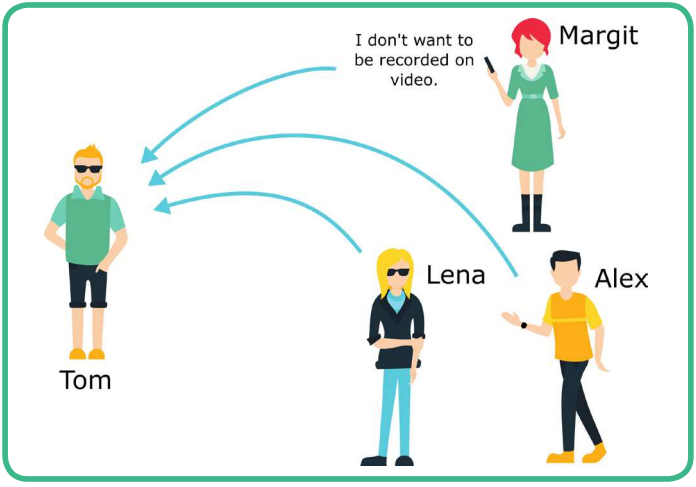
Responsibility: **Responsible Party**

Initiative

Who should take the initiative to initiate privacy mediation?

WHO?

The bystander(s)



Privacy mediating procedures can allow bystanders to actively approach a capturing system (here: Tom's data glasses), and request that their preferences are ensured (here: Lena who does not want to be recorded). The camera device responds accordingly (e.g., by notifying Tom or by stopping the recording). Communication could be initiated either automatically (e.g., as a broadcast to all devices in the immediate environment), manually, or in response to a request.

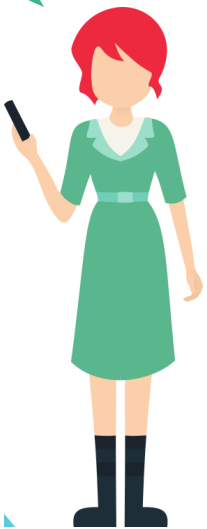
Communication

Initiative

Impulses

How would I define whether I want to be recorded or not? Do I need something to do so? Do I have to define privacy preferences? What if I don‘t?

There are cards to help you finding an answer to Margit’s questions. Have a look at these categories:



Communication: **Channel**

Participation: **Default Behavior**

Participation: **Timing**

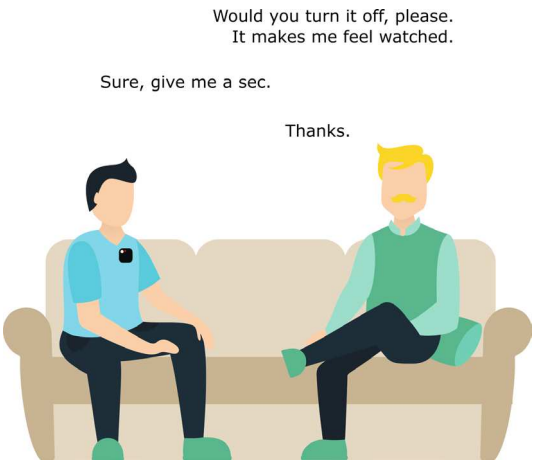
Participation: **Inclusion & Exclusion**

Channel

How is communication realized and which channels are used?

HOW?

Face-to-Face



In face-to-face communications, privacy preferences could be communicated both verbally, or non-verbally (e.g., through making a face). This is a very simple and convenient way of communication. However, device wearer and bystanders need to be able to understand each other, conflicting goals and preferences are difficult to resolve. Although there might be exceptions, face-to-face is typically a non-anonymous way of communication.

Communication

Channel

Impulses

What if I do not want to address the camera user in person? What happens if they do not comply with my request?

There are cards to help you finding an answer to Alex's questions. Have a look at these categories:

Enforcement: **Kind of Enforcement**

Enforcement: **Obligations**

Implementation: **Compliance**

Responsibility: **Responsible Party**

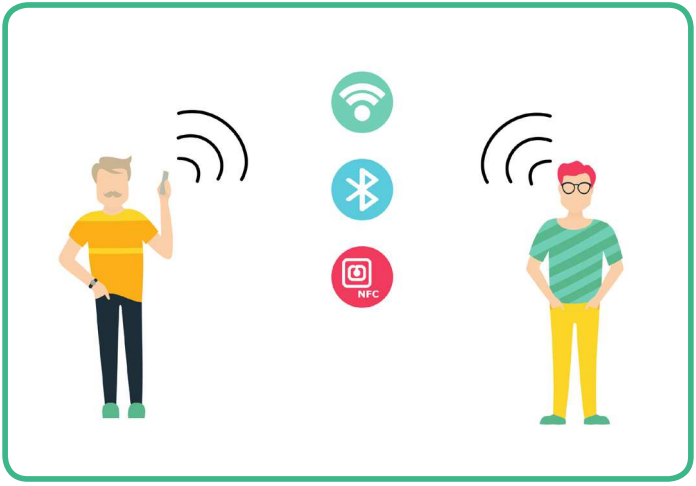
Communication

Channel

How is communication realized and which channels are used?

HOW?

Wireless-Signal-based



A camera device user and bystanders can exchange messages via wireless signals. There are multiple popular methods to communicate without a physical connection, e.g., WiFi, Bluetooth and BLE, and NFC. Thus, establishing a joint communication channel is fairly easy. However, when wireless signals should be used for communication, both, sender and recipient, need to possess a compatible device and be in range of each other.

Communication

Channel

Impulses

What do I have to do to encapsulate and send my privacy preferences in a wireless message? What if my smart phone is not compatible?

There are cards to help you finding an answer to George's questions. Have a look at these categories:

Implementation: **Parameters**

Participation: **Timing**

Participation: **Inclusion & Exclusion**

Participation: **Default Behavior**

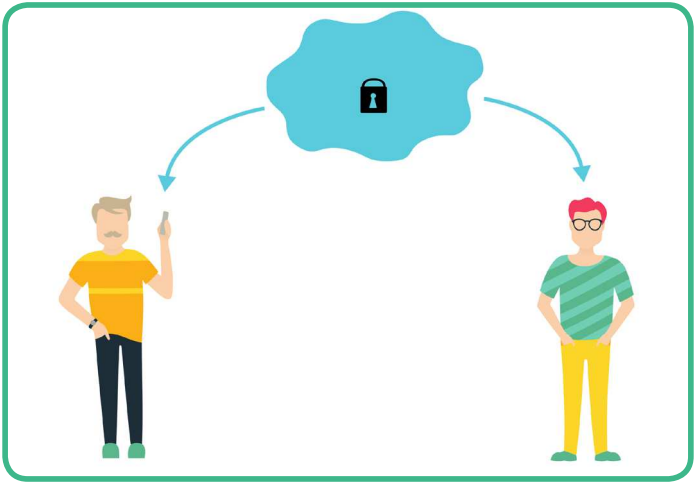
Communication

Channel

How is communication realized and which channels are used?

HOW?

Trusted 3rd-Party Service



Trusted 3rd-party-services can act as a mediator between camera device user and bystanders. Each of them communicates separately with the 3rd-party service, which, in return, notifies the other one about their preferences and actions. Depending on the nature of the 3rd-party service it might require some kind of identification, like a particular device or account.

Communication

Channel

Impulses

What if I want to use my smart glasses but not the 3rd-party service? Can the service provider see when and where I am using my smart glasses? Do I have to comply with all requests for privacy?

There are cards to help you finding an answer to Tobi's questions. Have a look at these categories:

Implementation: **Parameters**

Responsibility: **Responsible Party**

Enforcement: **Obligations**

Visibility: **Audience**

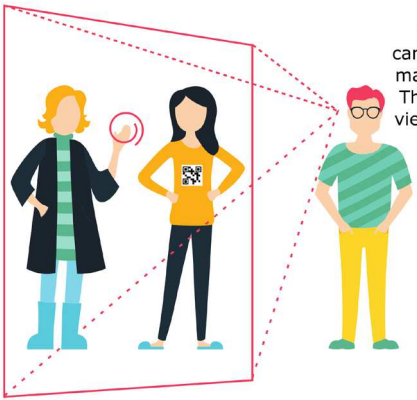
Communication

Channel

How is communication realized and which channels are used?

HOW?

Visual-Signal-based



Cameras perceive the world around them visually. In consequence, smart camera devices can react to visual markers (e.g., QR-codes, or patterns) or body movements (e.g., hand gestures). In addition, cameras might receive visual signals that their user cannot perceive, e.g., when wavelengths outside the human perception are used, such as near or far Infrared spectra.

Communication

Channel

Impulses

Do I need to provide an indication, if I want to be recorded, or do I have to signal that I don't? How can I know whether the camera has seen my signal?

There are cards to help you finding an answer to Marie's questions. Have a look at these categories:

Participation: **Default Behavior**

Participation: **Timing**

Visibility: **Audience**

Visibility: **Information Content**

Audience

To whom is the status of the camera visible?

To the user

A smart camera device might include manyfold functionalities. Not all of them necessarily require a camera stream, i.e., the camera itself does not need to be turned on, and may be deactivated. In this case, displaying the camera‘s status to the user means that they can tell at any time whether the device‘s camera is currently recording or deactivated.

Visibility

Audience

Impulses

When my smart glasses start recording, do I have to do ask bystanders for consent? If I unknowingly violate someone elses privacy, am I responsible for it?

There are cards to help you finding an answer to Tom's questions. Have a look at these categories:

Communication: **Initiative**

Enforcement: **Kind of Enforcement**

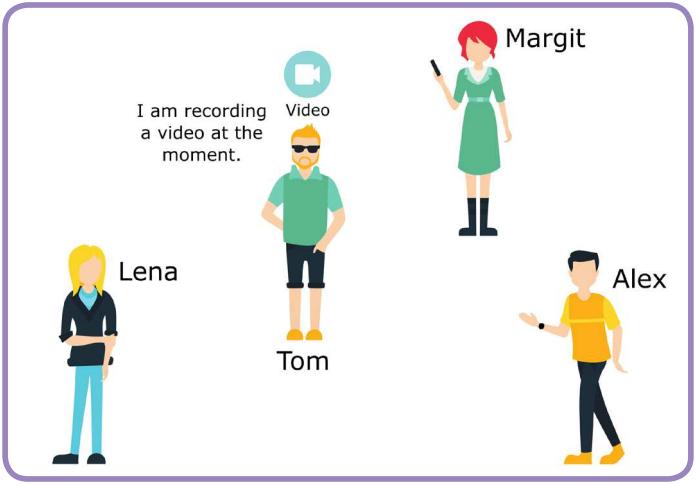
Responsibility: **Responsible Party**

Audience

To whom is the status of the camera visible?

TO WHOM?

To bystanders



Displaying the camera‘s status to bystanders means that they can tell whether the camera is recording or deactivated. This could be done using visual feedback on the device itself or by providing a “lookup” function on a bystander‘s device.

Visibility

Audience

Impulses

What if I do not understand, what the camera status display means? If I realize that someone is recording, can I do anything about it?

There are cards to help you finding an answer to Lena's questions. Have a look at these categories:

- Participation: **Default Behavior**
- Participation: **Timing**
- Participation: **Inclusion & Exclusion**
- Enforcement: **Obligations**

Audience

To whom is the status of the camera visible?

To third parties

Another option is to transmit the system‘s status to third parties (e.g., public authorities, operators of social networks); However, access might be restricted or limited. With this information third parties could prohibit the sharing of recordings if they infringe on the privacy of a person. Usage for law enforcement might also be possible.

Visibility

Audience

Impulses

Which kinds of information are visible to third parties? What may the collected information be used for? Could the collected information also be used for privacy protection?

There are cards to help you finding an answer to the anonymous user's questions. Have a look at these categories:

Visibility: **Information Content**

Enforcement: **Kind of Enforcement**

Enforcement: **Obligations**

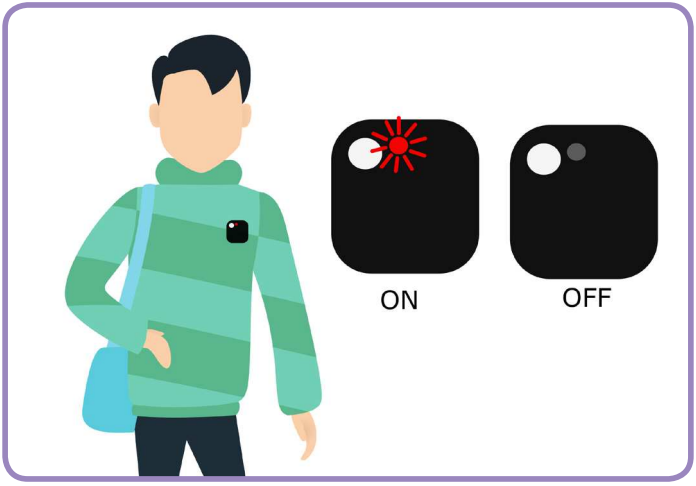
Implementation: **Parameters**

Information Content

What kind(s) of information does the camera‘s status display show?

WHAT?

Binary (ON - OFF)



A binary display of the camera status allows to derive whether the camera is switched on (“ON“) or turned off (“OFF“) . Information about what will happen with the recorded data, or whether and where the captured imagery is stored or shared is not provided.

Information Content

Impulses

Do I have to visibly show my camera‘s status? Who should see it? If someone else sees that my camera is turned on, and they object, can they force me to turn it off?

There are cards to help you finding an answer to Björn’s questions. Have a look at these categories:

Communication: **Initiative**

Visibility: **Information Content**

Enforcement: **Kind of Enforcement**

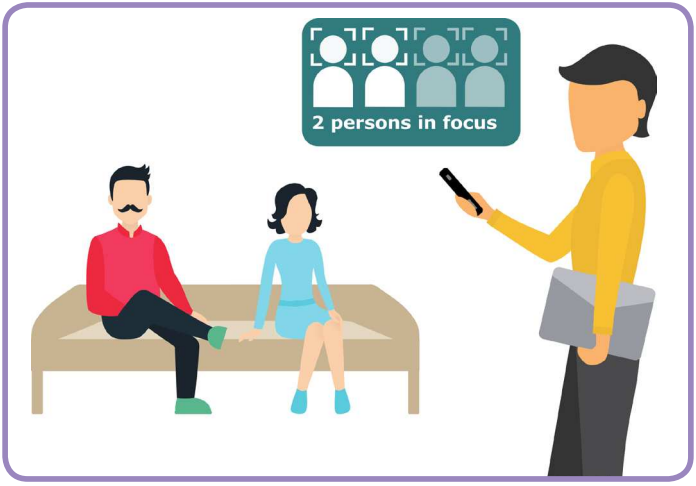
Enforcement: **Obligations**

Information Content

What kind(s) of information does the camera‘s status display show?

WHAT?

Content-based



A content-based display of the camera‘s status provides information about what is being recorded. It might differ between recordings without people in the picture (e.g., landscape) and recordings with one or more people in focus. This might be useful to the camera device user, but could also tell bystanders whether they are in the picture.

Information Content

Impulses

How does the camera react when bystanders are recognized in the frame? Would this affect how I can use my device? Can bystanders see that they are in the frame?

There are cards to help you finding an answer to Riley's questions. Have a look at these categories:

Participation: **Default Behavior**

Visibility: **Audience**

Enforcement: **Kind of Enforcement**

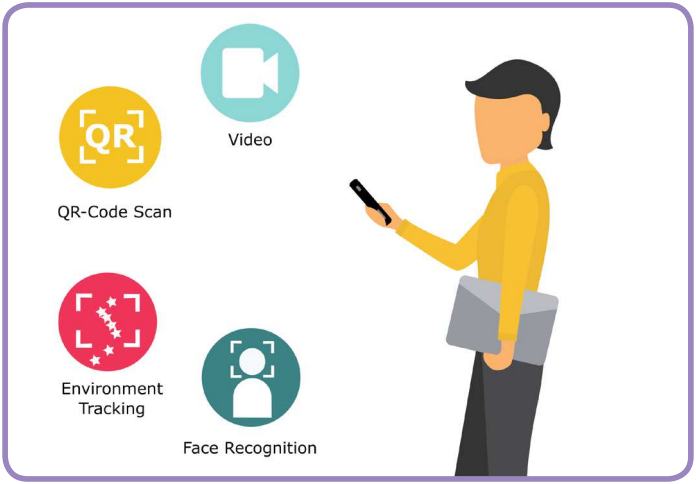
Enforcement: **Obligations**

Information Content

What kind(s) of information does the camera‘s status display show?

WHAT?

Intention-based



An intention-based display of the camera device‘s status provides information about the purpose or intention of the recording. Bystanders could be informed whether data is stored persistenty, e.g., for video recording, or looped, e.g., for tracking. For example, a status display could be placed as visual indicator on the camera device itself, displayed in the environment, or by providing a “lookup” function on a bystander‘s device.

Information Content

Impulses

Does it make a difference what I am using the camera for? Do I have to care about any bystander's privacy if I am using my camera for tracking and do not store any data?

There are cards to help you finding an answer to Riley's questions. Have a look at these categories:

Implementation: **Parameters**

Responsibility: **Responsible Party**

Enforcement: **Kind of Enforcement**

Enforcement: **Obligations**

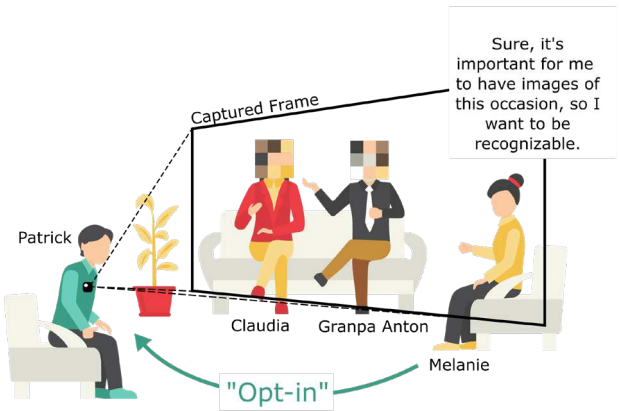
Participation

Default Behavior

What is the system‘s default behavior if a bystander is in the recorded frame?

WHAT?

Obfuscation



Obfuscation as the camera device‘s default behavior means that at first no one is identifiable, i.e., all faces are pixelated. Explicit agreement is required to capture a person. Therefore, Melanie informs Patrick’s lifelogging camera via a specified communication channel that she wants to be recorded by the camera. This is called “Opt-in”. Participants who, like Grandpa Anton, do not have access to this communication channel cannot communicate their consent.

Participation

Default Behavior

Impulses

How do I tell the system that I want to be recognizable on the recordings? Do I need a device for that? If I provided consent to a recording, can I withdraw it retrospectively?

There are cards to help you finding an answer to Melanie's questions. Have a look at these categories:

Communication: **Channel**

Participation: **Timing**

Participation: **Inclusion & Exclusion**

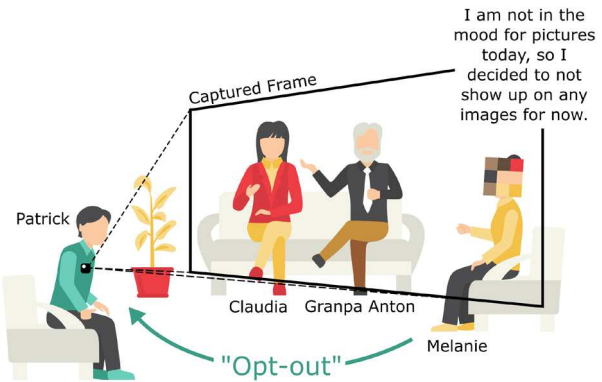
Participation

Default Behavior

What is the system‘s default behavior if a bystander is in the recorded frame?

WHAT?

No obfuscation



Smart camera devices could be configured in a way that by default everyone is identifiable. This default behavior is very similar to traditional, non-intelligent camera devices. Someone who does not want to be identifiable from the recordings has to inform via a predefined communication channel that they do not want to be recorded. This is called „Opt-out“.

Participation

Default Behavior

Impulses

How do I tell the system that I do not want to be recorded? When do I have to do that? If I decided that I want to be obfuscated, can I change my mind later?

There are cards to help you finding an answer to Melanie's questions. Have a look at these categories:

Communication: **Channel**

Participation: **Timing**

Participation: **Inclusion & Exclusion**

Implementation: **Compliance**

Timing

When can bystanders define if and by whom they would like to be recorded?

WHEN?

Before the recording

If privacy preferences are to be defined before the recording takes place, potential bystanders of smart camera devices (such as Marie) have to act proactively. They define all measures that are taken for their privacy protection, or by whom they would or would not like to be recorded beforehand. However, a system might also support revoking permissions, or changing preferences afterwards.

Timing

Impulses

How do I know that there are going to be recordings? Do I need a particular device or account to define privacy preferences? What if I do not define any? If I do, can I change my preferences later on?

There are cards to help you finding an answer to Marie's questions. Have a look at these categories:

Visibility: **Audience**

Participation: **Default Behavior**

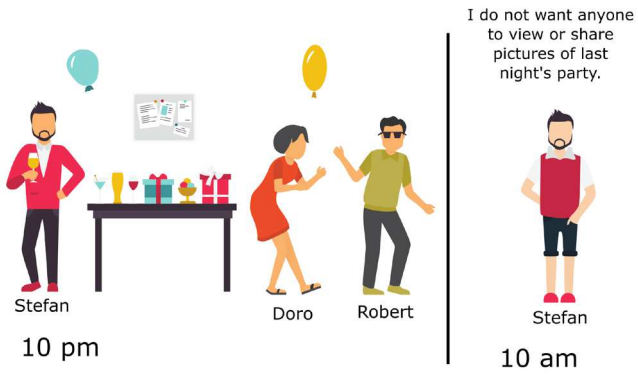
Participation: **Inclusion & Exclusion**

Timing

When can bystanders define if and by whom they would like to be recorded?

WHEN?

After the recording



The definition of privacy preferences might also happen reactively, in response to the recording. This could be done manually or automatically. It might involve asking the creator of the recording to delete images/videos or to restrict the access to the footage.

Timing

Impulses

How do I know that there are recordings of me being made? Do I need an account to tell the cameras who I am? What happens if images of me have already been shared, but I disagree with it?

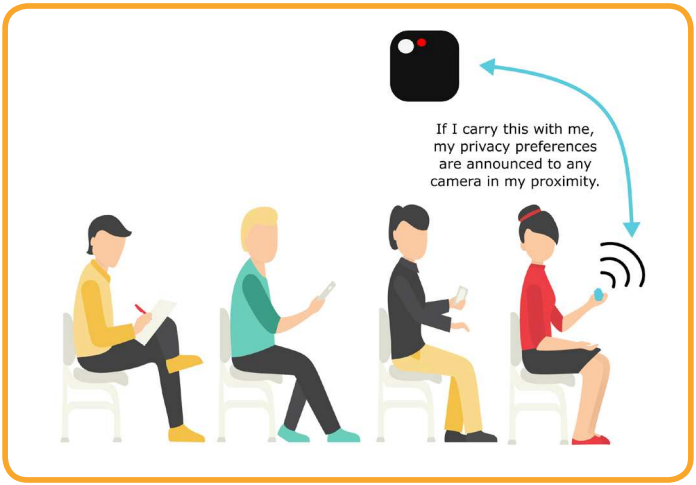
There are cards to help you finding an answer to Stefan's questions. Have a look at these categories:

- Implementation: **Parameters**
- Implementation: **Compliance**
- Communication: **Initiative**
- Enforcement: **Obligations**

Inclusion & Exclusion

Who can define if and by whom they would like to be recorded?

Physical artifact required



Physical artifacts could be used to communicate privacy preferences. Depending on the chosen communication channel the artifact might be a small transmitter of wireless signals, or a visually detectable marker. In any case, only those in possession of a compatible artifact or token can participate in privacy mediation.

Inclusion & Exclusion

Impulses

How does the physical artifact know about my privacy preferences? How do smart cameras detect the physical artifact/token? Do I need different tokens for different cameras?

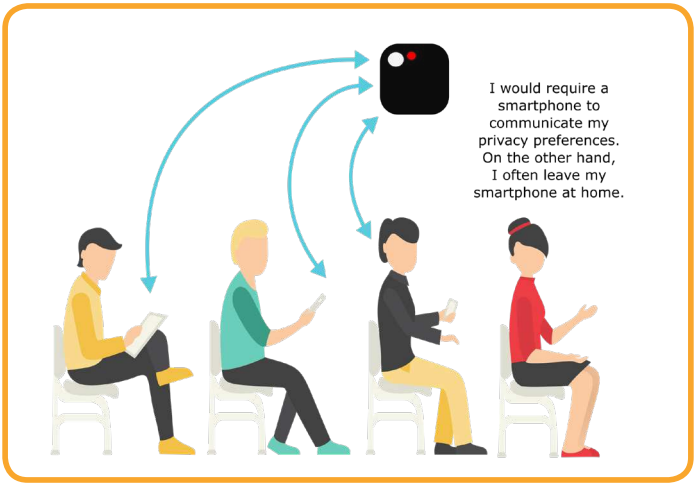
There are cards to help you finding an answer to Marie's questions. Have a look at these categories:

- Communication: **Initiative**
- Communication: **Channel**
- Implementation: **Compliance**
- Implementation: **Parameters**

Inclusion & Exclusion

Who can define if and by whom they would like to be recorded?

Smartphone required



Smart phones could also be used to communicate privacy preferences. In theory they are a special kind of physical artifact. However, in contrast to other options, they are already widely adopted and can access multiple channels of communication. Nevertheless, only those in possession of a compatible smart phone can participate in privacy mediation.

Participation

Inclusion & Exclusion

Impulses

Does my smartphone show me smart cameras in my proximity? Do I have to announce my privacy preferences to them? What if I don‘t do so?

There are cards to help you finding an answer to Marie’s questions. Have a look at these categories:

Visibility: **Audience**

Communication: **Initiative**

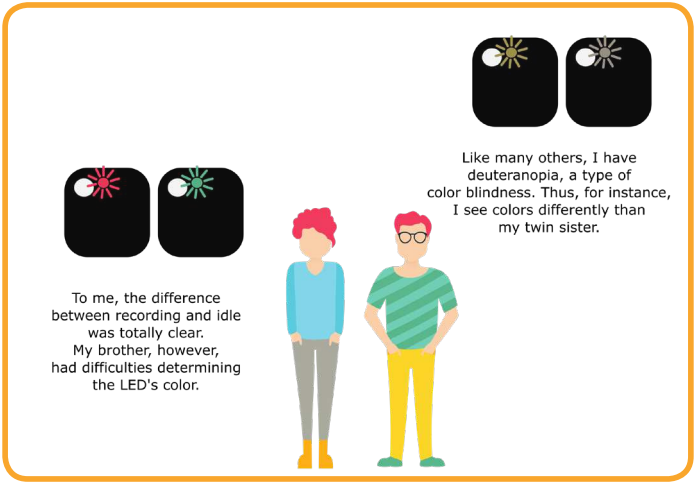
Communication: **Channel**

Participation: **Default Behavior**

Inclusion & Exclusion

Who can define if and by whom they would like to be recorded?

Accessibility



Accessibility is typically described as the ‘ability to access‘ a system or service. In this case, this means aiming to enable everybody to participate in privacy mediation. As everybody has a right to privacy, this is a very important goal. However, it is not always easy: the system should be accessible to everyone, regardless of age (e.g., elderly or children under age), disabilities (e.g., sight or motor impairments), or knowledge (e.g., language or reading).

Inclusion & Exclusion

Impulses

Accessibility is about more than color blindness! Does the system use communication channels that are accessible to everyone? Do you need particular skills to use it? Is there a fallback or alternative?

There are cards to help you finding an answer to Tobi's questions. Have a look at these categories:

Communication: **Channel**

Participation: **Default Behavior**

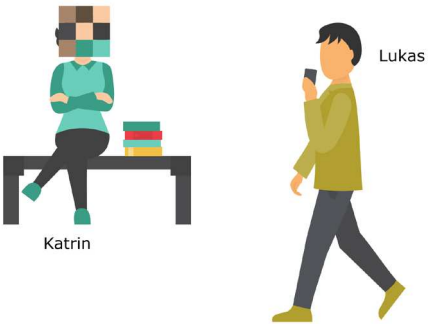
Responsibility: **Responsible Party**

Kind of Enforcement

How are privacy preferences enforced?

HOW?

Technically



The protection of privacy can be ensured through technical measures. These technical measures are typically applied by the system in reaction to communicated preferences or sets of rules. In the above example, Katrin's privacy is protected by "pixelating" her face. However, people might also be rendered invisible in pictures, or replaced by abstract avatars. Automatic deactivation of the camera is also a technical measure.

Kind of Enforcement

Impulses

Is everybody‘s face obfuscated by default or are there rules defining whose face will be?
When I am obfuscated in all those images, can this be reversed if I‘d like to appear in these images?

There are cards to help you finding an answer to Katrin’s questions. Have a look at these categories:

Participation: **Default Behavior**

Participation: **Timing**

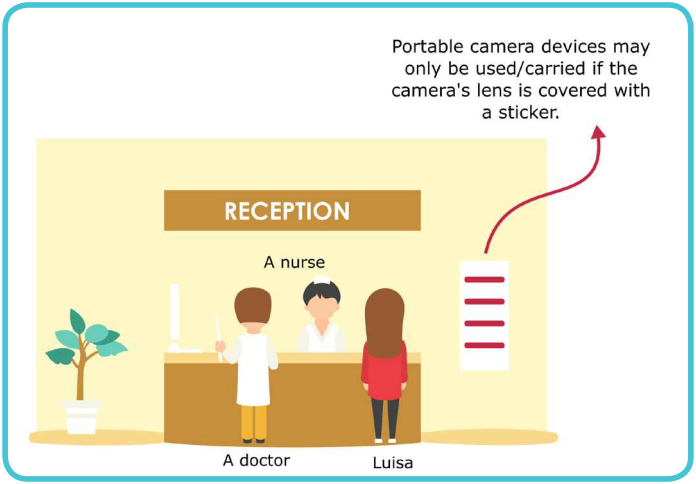
Implementation: **Parameters**

Kind of Enforcement

How are privacy preferences enforced?

HOW?

Physically



Unwanted picture or video recordings can be prevented by making the recording physically impossible. Carrying or using a device might be prohibited, or users might have to physically cover the lens, e.g., with tape. While physically covered lenses or enclosed devices are easy, trustworthy, and secure measures, there are various ways how no-camera rules might potentially be circumvented or fooled.

Kind of Enforcement

Impulses

Is everyone obliged to adhere to the no-cameras rule? Do I have to control whether all camera‘s are taped/turned off? How do I tell whether a camera is turned off?

There are cards to help you finding an answer to the nurse’s questions. Have a look at these categories:

Visibility: **Audience**

Visibility: **Information Content**

Communication: **Initiative**

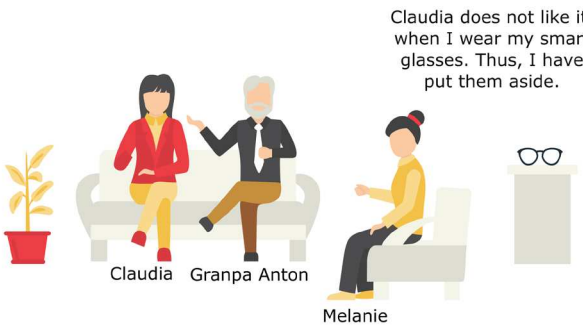
Enforcement: **Obligations**

Kind of Enforcement

How are privacy preferences enforced?

HOW?

Social Norms



If the recording is neither technically nor physically prevented, social or legal norms can protect the privacy of individuals (here Claudia and Granpa Anton). Melanie is not wearing her smart glasses when the others are around, because wearing them would be considered socially inadequate. However, it is her personal decision whether she complies with the social norm or defy the standards and accept possible consequences.

Kind of Enforcement

Impulses

How can I recognize that someone that I do not know does not want to be recorded? How do we define what is socially adequate usage behavior? Do I always have to stick to these norms?

There are cards to help you finding an answer to Melanie's questions. Have a look at these categories:

- Participation: **Default Behavior**
- Participation: **Timing**
- Enforcement: **Obligations**
- Implementation: **Compliance**

Obligations

In what way are measures for privacy protection brought to the user?

WHAT WAY?

Compulsory

If privacy protection is defined as compulsory, the user of the device can be forced to comply, e.g., with requests to deactivate their camera. Compliance can be enforced technically by the system (e.g., by prohibiting the recording or by pixelating faces) or by legislation (e.g., by threat of penalties).

Obligations

Impulses

Who decides what might be a potential infringement on privacy? How is the compulsory privacy protection implemented? Are there exceptions, like artistic freedom?

There are cards to help you finding an answer to Anne's questions. Have a look at these categories:

- Enforcement: **Kind of Enforcement**
- Implementation: **Compliance**
- Implementation: **Parameters**
- Participation: **Default Behavior**

Obligations

In what way are measures for privacy protection brought to the user?

WHAT WAY?

Suggested

Measures for protecting the privacy of others may be brought to the user of a device as a suggestion. This could be an automatically generated hint by the system, or both, a manual or automatic message from another participant who wishes to protect their privacy. The camera device user can then decide whether they would like to comply or not.

Enforcement

Obligations

Impulses

Do I have to adhere to privacy preferences defined by others, even if this is not obligatory? If I don't, would they be able to tell? Can bystanders see that I am doing recordings?

There are cards to help you finding an answer to Lena's questions. Have a look at these categories:

Responsibility: **Responsible Party**

Implementation: **Compliance**

Visibility: **Audience**

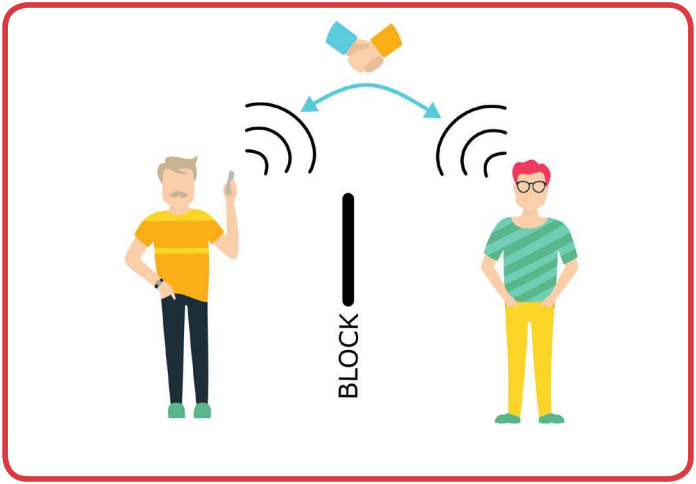
Visibility: **Information Content**

Compliance

Who gets the final say in implementing privacy protection?

WHO?

Compliance-dependent



In general, compliance-dependent privacy protection is based on a mutual agreement between two parties. The two parties (here: Tobi and George) might agree verbally to turn off the camera device's recording. If devices are used for communication, privacy protection is only ensured, when the recording device (here: smart glasses) is compatible with the device requesting privacy (here: smart phone) and respects the request, e.g., because its user configured this behavior.

Implementation

Compliance

Impulses

How can I determine whether I want to be recorded or not? Do compatible devices have to comply with my privacy preferences? Is there a fallback solution in case my device is not compatible?

There are cards to help you finding an answer to George's questions. Have a look at these categories:

Participation: **Default Behavior**

Enforcement: **Obligations**

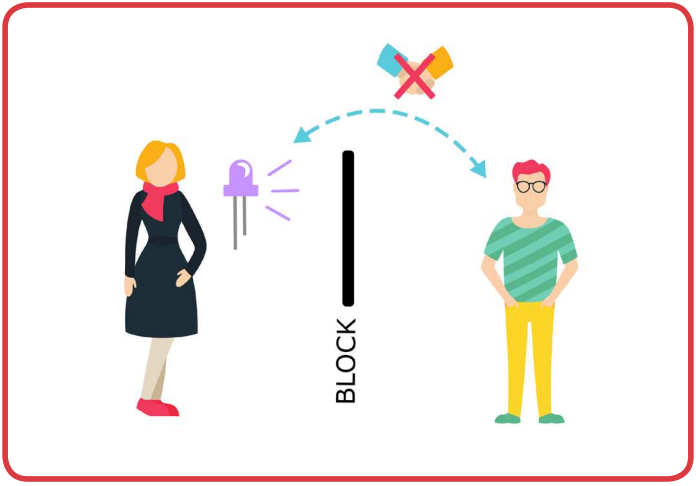
Enforcement: **Kind of Enforcement**

Compliance

Who gets the final say in implementing privacy protection?

WHO?

Compliance-independent



Some technologies can actively prevent the recording by a camera device without the need for cooperation or agreement with the device user. For example, infrared light or retroreflective materials can be used for this purpose. The advantage of these systems is that they do not require any compatibility compliance.

Implementation

Compliance

Impulses

In what way can I restrict recordings I do not want? Do I need a device for this? Are there locations where devices that could block recordings should not be used or are forbidden?

There are cards to help you finding an answer to Anne's questions. Have a look at these categories:

- Enforcement: **Kind of Enforcement**
- Communication: **Channel**
- Participation: **Inclusion & Exclusion**
- Responsibility: **Responsible Party**

Parameters

Which parameters define privacy protection?

WHICH?

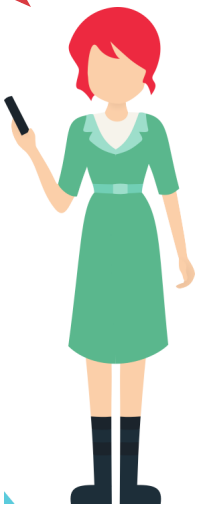
Location-based

The recording by a device can be restricted according to location-based rules. Location-based means that camera recordings are prevented in a certain room, building or area. Restriction of use can be enforced through social norms, no-camera rules or by technical measures (e.g., radio signals).

Parameters

Impulses

Can anyone who owns a place restrict recordings? How could they enforce that no unauthorized recordings are made? In what way would the recording be restricted?



There are cards to help you finding an answer to Margit's questions. Have a look at these categories:

Participation: **Default Behavior**

Enforcement: **Kind of Enforcement**

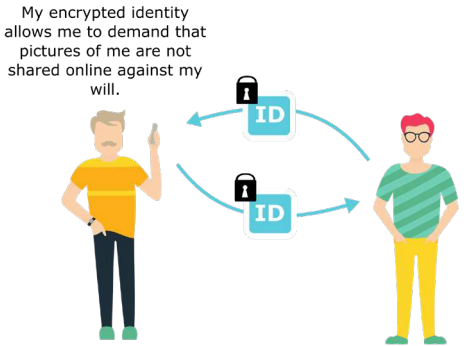
Enforcement: **Obligations**

Parameters

Which parameters define privacy protection?

WHICH?

Identity-based



Privacy protecting measures can be tied to the identities of both user and bystander. Bystanders could define by whom they would like to be recorded or not. As with analogue photography, this is easy when everyone is known to each other. However, technically supported exchange of (anonymous) identities (e.g., while co-located), can also be used to enable deletion or access restriction at any time after recording or publication.

Implementation

Parameters

Impulses

How do my smart glasses know who wants to be recorded and who does not? Do they send signals or messages? In what way are my recordings restricted?

There are cards to help you finding an answer to Tobi's questions. Have a look at these categories:

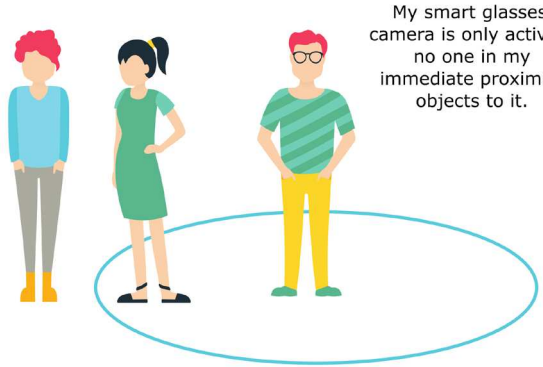
- Communication: **Channel**
- Participation: **Timing**
- Participation: **Inclusion & Exclusion**
- Enforcement: **Kind of Enforcement**

Parameters

Which parameters define privacy protection?

WHICH?

Proximity-based

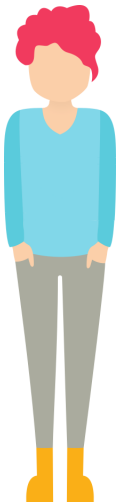


Proximity-based methods use a predefined perimeter around a device (in this case smart glasses) within which certain rules are applied. E.g., privacy preferences of people in the user‘s immediate environment (e.g., the same room) are considered, preferences of people in wider periphery (e.g., the same building) are not considered.

Parameters

Impulses

Do I need a device to be detectable? How is the radius of immediate proximity defined? Do I have to announce that I do not want to be recorded?



There are cards to help you finding an answer to Tina's questions. Have a look at these categories:

Communication: **Initiative**

Communication: **Channel**

Participation: **Inclusion & Exclusion**

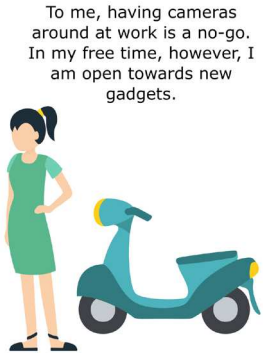
Parameters

Which parameters define privacy protection?

WHICH?

Time-based

9am - 12pm, 2pm - 6pm.



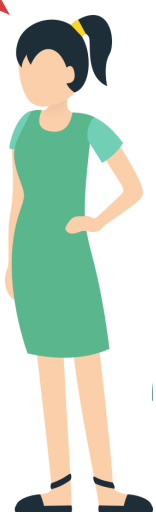
12pm - 2pm, 6pm - 9am.

Privacy preferences might depend on the time of the day. They might also be different on the weekend than during the week. In consequence smart camera devices might consider timing as part of a person's privacy preferences or as general sets of rules.

Parameters

Impulses

Do I define the times when I'd like recording to be restricted or do I define when recordings are ok? Do I have to inform others about these preferences? How can I do so?



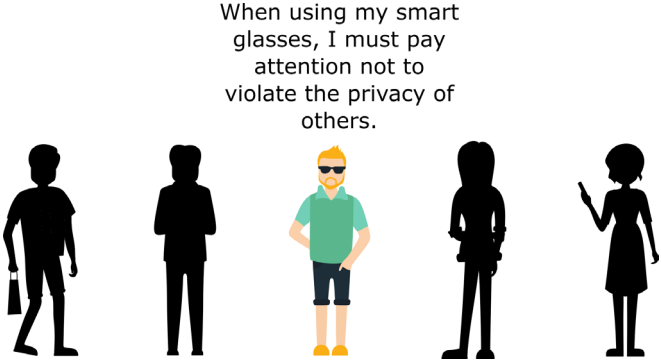
There are cards to help you finding an answer to Lauren's questions. Have a look at these categories:

- Participation: **Default Behavior**
- Participation: **Timing**
- Communication: **Channel**
- Communication: **Initiative**

Responsible Party

Who is responsible for protecting the privacy of third parties?

The device user



When the user is responsible for the privacy protection of third parties, it‘s their obligation – like when using a conventional camera – to adapt the use of the device to the situation, to obtain consent and, if necessary, check every recorded image before uploading it to a cloud or to a social media website. However, this can be difficult with large numbers of images or real-time applications. Therefore, the user could be supported by various existing or future technologies.

Responsibility

Responsible Party

Impulses

I have trouble keeping the overview: is there any tool that can assist me in keeping track of other's privacy preferences? How do I know that there is someone who might oppose to my smart glasses?

There are cards to help you finding an answer to Tom's questions. Have a look at these categories:

- Communication: **Initiative**
- Communication: **Channel**
- Enforcement: **Kind of Enforcement**
- Implementation: **Parameters**

Responsible Party

Who is responsible for protecting the privacy of third parties?

WHO?

Everyone individually

In terms of my privacy, I feel better, if I am taking care of protecting it myself.

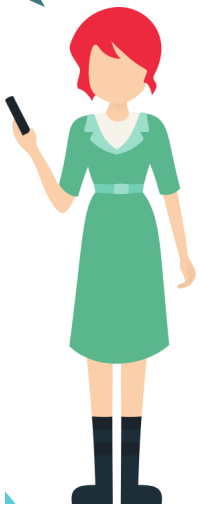
Responsibility for the protection of privacy could also be distributed equally amongst users and bystanders. As an individual can assume both roles simultaneously, e.g., if everyone would have a smart camera, everyone could (potentially) be user and bystander at the same time. To deal with this situation, appropriate mechanisms and technologies that realize privacy mediation can be made available.

Responsibility

Responsible Party

Impulses

I might be user and bystander of a smart camera at the same time. Which options do I have for protecting my privacy and which for the privacy of bystanders? How is privacy protection enforced?



There are cards to help you finding an answer to Margit's questions. Have a look at these categories:

- Communication: **Initiative**
- Communication: **Channel**
- Enforcement: **Kind of Enforcement**
- Participation: **Default Behavior**

Responsible Party

Who is responsible for protecting the privacy of third parties?

WHO?

The manufacturer

The manufacturer can take responsibility for ensuring the privacy of third parties by providing mechanisms which actively contribute privacy protection. Any actions of the user which (potentially) violate the privacy of third parties could be prevented through appropriate software or hardware. However, this may also limit functionality. Certification of devices which protect privacy could also be possible.

Responsibility

Responsible Party

Impulses

How could my company implement and enforce privacy protection? How can it be guaranteed that my company's privacy protection is not circumvented?

There are cards to help you finding an answer to the manager's questions. Have a look at these categories:

Enforcement: **Obligations**

Enforcement: **Kind of Enforcement**

Implementation: **Compliance**

Responsible Party

Who is responsible for protecting the privacy of third parties?

Legislation

Legislation can take actions at different levels to prevent intrusion of privacy by smart cameras e.g., by enforcing limitations and restrictions of use, certification of equipment and manufacturers, or import regulations, etc. However, it is important that laws and regulations always have to be enforceable and that they are not limiting the fundamental rights of the individual.

Responsibility

Responsible Party

Impulses

How is it ensured that regulations are not avoided or circumvented? What about different rights (e.g., privacy vs. freedom of art) that need to be balanced against each other?

There are cards to help you finding an answer to the anonymous user's questions. Have a look at these categories:

Enforcement: **Obligations**

Enforcement: **Kind of Enforcement**

Implementation: **Compliance**