Smart Privacy Visor: Bridging the Privacy Gap

Adrian Dabrowski[1], Katharina Krombholz[1], Edgar R. Weippl[1], and Isao Echizen[2]

[1] SBA Research, Vienna, Austria,
(adabrowski|kkrombholz|eweippl)@sba-research.org
[2] National Institute of Informatics, Tokyo, Japan
iechizen@nii.ac.jp

Abstract. Due to the propagation of devices with imaging capabilities, the amount of pictures taken in public spaces has risen. Due to this, unintentionally photographed bystanders are often represented in pictures without being aware of it. Social networks and search engines make these images easier accessible due to the available meta-data and the tagging and linking functionality provided by these services. Facial recognition amplifies the privacy implications for the individuals in these pictures. Overall there exist three main classes of wearable picture-related Privacy Enhancing Technologies (PETs). As they need different prerequisites to operate and become effective they have unique time frames in the future where they can be effective even if introduced today. The group of *face pattern destroying picture PETs* work directly against current face detection algorithms and is the choice for immediate usage. These PETs destroy face patterns and inhibit the detection and automated processing and meta-data enrichment of individuals. This unconditionally visual destructive behavior can be a major obstacle in transition to other PETs. In this paper, we describe how to master a smooth transition between these classes including the restoration of the visual damage some of these methods entail. Furthermore, we propose the *Smart Privacy Visor*, a PET which combines the previously published *Privacy Visor* and the *Picture Privacy Policy Framework*. The overall goal of this transition is to create a PET that avoids identifiable and linkable properties which contradicts the goals of picture PETs in the first place and offer a visually appealing photographic result at the same time.

Key words: privacy invasion, involuntary photographs, unintentional photographs, picture privacy, privacy policy

1 Introduction

Portable and wearable imaging devices such as mobile phones and Google Glass are a privacy threat of the current decade. Most of them offer discrete recording capabilities, which make collecting, sharing, and publicizing images and videos easier than ever. All these potentially infringing privacy of involuntarily or unintentionally photographed individuals. This is maximized by meta information collected alongside these images (e.g. name tagging, automatic face recognition,

geo information tags,...) and then linked to online profiles or indexed by search engines.

The online sharing of personal information in the age of user-generated content without the pictured individuals' consent can change the lives of these individuals in a very negative ways. Thus, the concept of individual privacy has not only been changed, but also requires new tools and regulations to close the communication gap between photographers and recorded bystanders. Recently, a number of Privacy Enhancing Technologies (PETs) has been proposed in scientific publications to address this challenge. Some do not require any infrastructure or changes to the status-quo and work solely by circumventing current state of the art face detection, recognition, and processing algorithms. These can be used right away but have visual and functional limitations [1–5].

Some propose enforcement by automatic privacy filters at online social networks and other publication sites that detect visual clues, markers, or codes that a particular person has to wear or show [6–9]. These techniques are easy to integrate in current online systems by software updates at the major operators. These operators (e.g. Facebook, Google) would need an incentive to do so, e.g. public pressure or legislative changes. These systems can start operating within months, once agreed upon. They offer finer privacy control for the affected people but have a certain degree of complexity.

Other solutions require software and hardware updates to current imaging devices [10–12]. Software updates (e.g. for receiving and decoding light impulses) can be rolled out by vendors for wearables, mobile phones and even digital cameras. However, hardware updates (e.g. adding an RFID receiver [13–15]) would require a whole new camera generation to replace the existing ones. Even if mandated by law and introduced for all new cameras from today, this will take several years before the natural camera lifetime would force customers to replace cameras. These PETs potentially offer the best usability for the photographed person as they are shaped by fully developed user interfaces in a best-case working scenario.

Every of the above picture PET classes has their own time-to-market constrains and can therefore be set into a deployment time line. In this paper we analyze the situation and propose a novel transition mechanism that will allow seamless usage throughout the different generations of these PETs.

The paper is structured as follows: In Section 3 we describe the currently available picture PETs and in Section 4 discuss why this situation is unsatisfying. We argue that a transition solution is necessary and how it works in Section 5 and in Section 6 present the concept of the *Smart Privacy Visor*. We conclude with Section 7.

2 Motivation and Background

Many countries define rights regarding a person's own image. However, they are neither easy for a photographed person to enforce, nor for the photographer to follow. The image of a person might have been unintentionally captured by a photographer without the person noticing that his/her picture was being taken, the person may simply not know the photographer, or the person may not know

when and where his/her picture was published and in which context. This lack of knowledge can hinder the person from exercising his/her legal rights. Moreover, the person has no way to inform potential or actual picture takers of their self-chosen restrictions on how their image shall be handled.

Likewise, a conscientious photographer might not have the chance to ask all the people whose image he/she captured for their consent to use their images. In any case, the persons right to control how his/her image is used is lost due to a gap in the communication and control path from the person to the photographer and/or publisher of the photo. Additionally, different countries regulate this right differently: some tie it to the act of publishing the picture while others tie it to the act of taking the picture.

Several picture PETs have been proposed recently (Table 1), which are roughly categorizable into three classes that resembles to three generations because of differences in the *time to market* - i.e. the time these technologies could be rolled out and be effective, if started today. On the other hand, picture PETs that can be used starting now have weaknesses in functionality, social acceptance, and or usability. Therefore we anticipate, that usage of these technologies will proceed in stages or generations. Therefore, establishing a viable and smooth update path is of importance.

It is important to notice, that picture PETs don't only serve the privacy concerned or photo shy citizen, but also provides legal certainty for professional users such a photographers, professional picture databases, and publishing companies.

3 Picture PET Systematization

In this Section we categorize currently available or proposed picture PETs. An overview is given in Table 1. These PETs have typically been presented for either (single) still images (S), (mobile) video (V), or stationary CCTV (C). In general, when a PET is capable to handle still images, it can be also used for the other two purposes: $S \supset V \supset C$. However, not vice versa: a PET designed for Closed Circuit Television (CCTV) typically requires stationary cameras. CCTV only PETs have been included for completeness. They are designed for single operator systems with a limited geographical area and number of users. Still, they can give some ideas for similar *wearable* picture PETs.

3.1 Face Pattern Destruction Picture PETs

This class of PETs is based around prohibiting the automatic detection of faces in photographs. Lightweight face detection mechanisms are typically employed as first step in an image processing chain, to locate face candidates before running computationally more expensive algorithms (such as recognition) on them.

Simply by removing the face from the automated processing chain at the very first step, prohibits its automatized processing facilitating naming, indexing, linking, and tracking. Some social networks and other publishing platforms still have the possibility of manually marking a face and adding a name tag. However, this requires deliberately actions by the uploader or publisher and is much more

Table 1: Comparison between available or proposed picture PETs

Name	Author	Type	Still image / Video / CCTV	Active artifact on user side	Camera can be mobile	Decode form/for single image	Online connection	Peer to Peer communication	GPS required	Radio RX on camera	Radio TX on camera	Central clearing or database entity	Face Pattern Destruction	Face or biometric database	Person identification for privacy	Visibility[1]	Settings change effort[1]	Number of settings	Dimensions of settings	Overall complexity of settings[1]
CV Dazzle	Harvey,2010	Hair and makeup	SVC	-	+	+	-	-	-	-	-	+	-	-	5	5	2	1	1
IR Privacy Visor	Yamada,2013	Infrared pattern destruction	SVC	+	+	+	-	-	-	-	-	+	-	-	2	1	2	1	1
Pasv. Privacy Visor	Yamada,2013	Visual pattern destruction	SVC	-	+	+	-	-	-	-	-	+	-	-	3	2	2	1	1
Blind Spot	Patel,2009	Detect lens, blind camera	SVC	+	-	/	-	-	-	-	-	-	-	-	2	2	2	1	1
P3F	Dabrowski,2013	Cloth pattern & accessories enc.	SVC	-	+	+	-	-	-	-	-	-	-	-	2	3	40	4	4
Respectful Cameras	Schiff,2007	Visual mark. (color of hat/vest)	SVC	-	+	+	-	-	-	-	-	-	-	-	4	3	2+	1	1
OfflineTags	Palles,2014	Visual markers (buttons)	SVC	-	+	+	-	-	-	-	-	-	-	-	3	2	4	1	1
Do Not Share	Ashok,2014	Infrared beacons, data TX	(S)VC	+	+	-	-	+	-	-	-	-	-	-	2	2	4	1	1
Hand Gestures	Barhm,2011	Hand gestures	VC	-	+	-	-	-	-	-	-	-	-	-	2	1	3+	1	2
Privacy Mgmt.	Halderman,2004	XOR computational consent	any	+	+	+	+	+	-	-	-	-	-	-	0	1	–	–	–
FaceBlock	Yus,2014	Eigenface & policy via Bluetooth	SVC	+	+	+	-	+	-	+	+	-	-	-	+	0	2	2	1	1
Snap Me	Henne,2013	GPS & face DB clearinghouse	SVC	+	+	+	+	-	+	-	-	+	-	+		0	2	2	1	1
PED Cloak	Brassil,2005	Mobile phone app	(S)V(C)	+	+	+	+		+	+	+	+	-	-	+	0	2	2	1	1
(no name given)	Wickramasuriya	RFID	C	+	-		-	-	-	+	+	+	-	-	+	0	3	2	1	1
PriSurv	Chinomi,2008	RFID with signal strength	C	+	-		-	-	-	+	+	+	-	-	+	0	3	2	1	1
(no name given)	Moon,2009	RFID with visual tracking	C	+	-		-	-	-	+	+	+	-	-	+	0	3	2	1	1

[1] Scale from 0 to 5: 0..none, 5..most

unlikely to occur. It will also inhibit the automated processing through any third party service such as search engines.

Contrary to obvious assumption, simply wearing sun glasses is not sufficient for the destruction of the patterns used for face detection. For this, several different solutions exist. *CV dazzle* [1] (Figure 1a) uses distinctive makeup and hair style to outsmart face detection. The flashy look might not be socially accepted in all situations and is a lot of work to maintain.

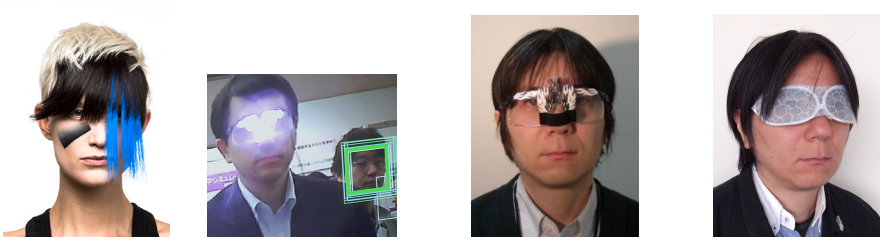
The infrared *Privacy Visor* [2, 3] depicted in Figure 1b are goggles with mounted infrared LEDs. Their light is not visible to the naked eye but to most cameras. However, recently, cameras are getting better and less sensitive to infrared. A second generation of Privacy Visor [4] used patterns around the eye part to distract face detection algorithms. The third version of Privacy Visor uses a more stylish approach by resembling white sunglasses.

In contrast, *Blind Spot* [5] uses image recognition to find camera lenses and temporarily blind them with laser beams. The large amount of hardware needed for this approach does not make it portable.

All face processing inhibiting PETs have in common, that their visual impact is quite high. If not already in real life, than at least on the digital image (e.g. by infrared, laser). Therefore, a lot of image information is actually destroyed in the process. Changing privacy settings is particularly complicated with CV Dazzle.

3.2 Visual Encoding Picture PETs

Visual encoding the privacy information has the advantage of not needing any new hardware. In best case, changes are only necessary in publishing systems or



(a) CV Dazzle (b) IR Privacy Visor 1 (c) Privacy Visor 2 (d) Privacy Visor 3

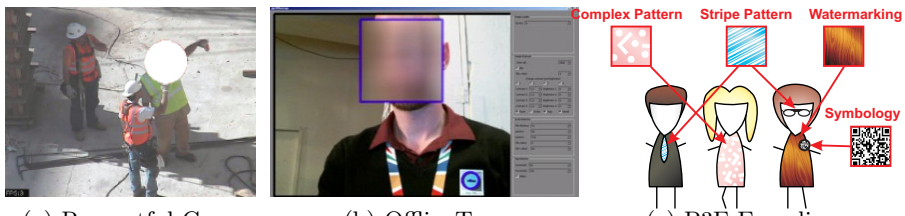
Fig. 1: Examples of face pattern destruction PETs [1, 3, 4]

in the camera software. This ease the introduction of those systems. The visual impact of these systems is moderate to minimal: they can be disguised as normal fashion or covers only non essential parts of an image (e.g. buttons on a jacket).

Respectful Cameras [6], *Picture Privacy Policy Framework* (P3F) [7], and *OfflineTags* (OT) [8] use visual markers attached to the subjects. Respectful Cameras simply uses the color of vests and or hats. They are quite visible and primarily usable in an controlled environment, such as employees in a museum or at a construction site. P3F tries to hide the markings into subtle patterns such as stripes, dots, colors, or with watermarking technologies besides symbols on accessories. This gives this PET the ability to encode a very fine granulated restriction policy (total 40 combinations in multiple dimensions). OfflineTags offer four settings with large wearable buttons not trying to hide its existence from the human spectator.

This kind of wearable visual encoded picture PETs have the drawback, that the effort to change privacy settings is between moderate and high. Changing cloths in public is not always easy. P3F tries to encounter this, by allowing easier changeable wardrobe and accessories to override bulkier and hard to change wardrobe like shorts, shirts, or jackets by encoding priorities. However, preliminary results of our own usability study show that users prefer a less complex solution.

Do Not Share [16] uses the infrared sensitivity of CCD and CMOS sensors [2] to transfer the policy from the subject to the camera as light pulses. While this can be implemented on a camera or a smart phone as software update, it does require to record a sequence of images to decode the serial data even if only one



(a) Respectful Cam. (b) OfflineTags (c) P3F Encoding

Fig. 2: Examples of visual encoding picture PETs

still image is taken. Barhm et al. [9] has a similar limitation for decoding hand gestures and signes, but is designed for video streams and CCTV systems.

3.3 Secondary Channel Picture PETs

A secondary channel is another way of communication between a subject and a photographer. This might by a local wireless signal or an Internet connection. In most cases this implies new sensors or transmission modules for cameras. In some cases it can be implemented only in software for devices that are already equipped with an Internet connection, such as mobile phones and wearable computers. In general, it requires a whole new generation of devices.

Adding an additional communications channel is a classic solution for closed systems (in terms of users and area). A couple of authors [13–15] suggested using RFID to identify users and/or their privacy settings. This was intended for CCTV systems and is only partly transferable for open public use. In many cases, it just generates a new unique identifier that contradicts the privacy interests of the user.

Snap Me [10] takes a similar approach by communicating the geographic position and orientation of all of its users and cameras to central clearing house. An optional biometric face database can improve the detection of the subjects in question further to finally anonymize them. However, this solution implicitly creates a huge surveillance infrastructure. Brassil [11] suggests a similar solution but as a mobile phone application only. *FaceBlock* [12] implemented a Bluetooth protocol on Google Glass that broadcasts the owners Eigenface template and the privacy policy to all other devices nearby. The photographing device can use this template to uniquely identify the subjects and apply the appropriate policy.

3.4 PET Generations

Every of the above picture PET classes has their own distinct *time-to-market* (i.e. time it is deployable and becomes effective) constrains and can therefore be set into a deployment time line (Figure 3).

Face pattern destructive PETs do not require any prerequisites in form of infrastructure, changes to current cameras, or legislation. They can be used right away. We will call them *1st generation picture PETs*. Note, these PETs have a strong visual impact on the image itself, unlike the other classes.

Most *visual encoded PETs* can be implemented by a software update in publishing websites such as social networks. While their operators might need to be forced by public opinion or legislation, an implementation could go live within months. For cameras, when implementable in software only, such updates (e.g. for receiving and decoding light impulses) can be rolled out by vendors for digital cameras, mobile phones and wearables. More likely, such updates will only reach the latter two in significant numbers.

The *third generation* solutions require software and hardware updates to current imaging devices. This includes most solutions with a secondary channel. A new hardware element (sensor, transmitter) to become usable requires a whole new camera generation to replace the existing ones. Even if mandated by law and

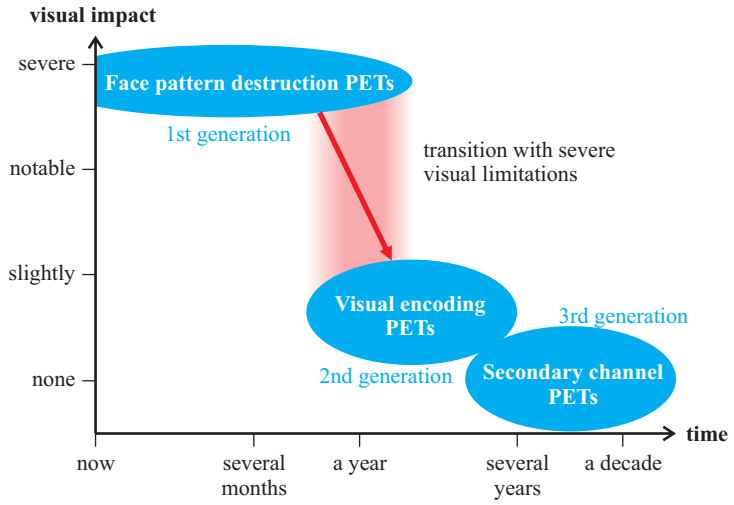


Fig. 3: Time for picture PETs before they become effective, if introduced today vs. visual destruction; apx. log scale

introduced for all new cameras from today, this will take several years before before the natural camera lifetime would force customers to replace their cameras. However, these PETs potentially offers the best usability for the photographed individual.

4 The PET Generation Gap

In general, we anticipate that users will move to higher generation picture PETs because of their increased usability, but can only use what is available and functional at that time. This makes a smooth transition between the generations essential. Thus, for a extended time, privacy aware users will have to use more than one PET or a transitional PET sitting between these generations. When a certain generation is not supported in the publishing process, the proceeding PET generation will take over. The main differences between the classes are:

Enforcement Unlike 1st generation PETs, all following generations need some sort of explicit support at the imaging or publishing site of the publishing processing chain. Therefore, 1st generation PETs can serve as fallback in situations where other privacy protecting schemes are not in effect. Their enforceability is comparable to the *Robots Exclusion Standard* [17] on the world wide web, also known as *robots.txt*.

Functionality Many 2nd and 3rd generation PETs (e.g. [7,8]) offer fine granulated privacy settings. A typical fallback scenario to the 1st generation PET will typically mean inhibiting face processing completely, but allowing some usages for publishing sites which support higher generations.

Visual Impact Face pattern destructive PETs inhibit the detection and the potentially exposing processing by destroying the face patterns. As shown in Figure

1, this has a severe visual impact. Allowing some picture usages for publishing systems with support for 2nd or 3rd generation privacy protection implies, that this destructive behavior needs to be reverted to offer visual appealing images (Figure 3). This is also an incentive to support higher generation PETs.

4.1 Transition for 1st generation to 2nd or 3rd generation

As mentioned in Section 3.1, 1st generation picture PETs work by destroying face patterns and therefore omitting potentially privacy post-processing of the person and its meta information. This is usually achieved by visually modifying or even occluding significant parts of the face. In such a scenario, a 2nd generation PET therefore meets the following challenges:

– The face is not visually appealing for the viewer, even when the 2nd generation policy partly allows its usage. The amount of visual damage can be quite severe. Therefore, the face and potentially other parts needs to be visually reconstructed.
– The face might not be easily found automatically (this was what the 1st generation PET intended) and attached to a body. However, this is necessary in many systems, to correctly attach and apply the correct privacy policy for this particular person in a picture.

These unique challenges and possible solutions are described in Section 5.

4.2 Transition from 2nd generation to 3rd generation

These PETs do not occlude or impair the visual appearance of a person significantly. The transition does not provide any additional challenges despite potentially conflicting policies. In which case precedence to the higher generation should be given, as it usually provides the best usability.

5 Bridging the Gap - A Smooth Transition

The following section describes in detail the mechanisms as needed for a smooth transition from 1st to 2nd generation picture PETs. Figure 4 drafts how the current 2nd generation image processing pipeline (white) has to be extended by a second pipeline (gray) to handle 1st generation transitional PETs.

The transition mechanism has to provide the 2nd generation with the following functionality.

– Neutralize the partly destructive and invasive image modifications of 1st generation picture PETs.

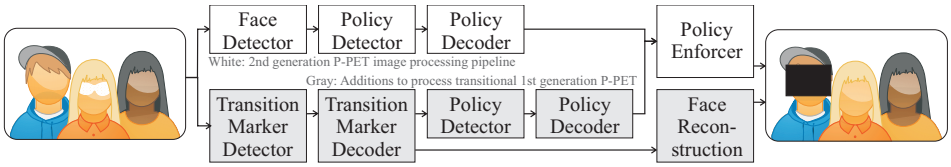


Fig. 4: Transition aware decoding including face reconstruction (additions in gray)

– Offer the 2nd generation algorithm clues where to find the face and what its orientation is (for reconstruction)
– Provide enough information to actually reconstruct the face.
– Optionally include the 2nd generation privacy policy, with the 1st generation's setting as fallback.

5.1 Reconstruction of Face

Reconstruction of the occluded or dazzled face is one of the most challenging tasks for a transitional PET. Many face reconstructing algorithms have been solely developed for the case of feeding the outcome into an biometric face identification system. Therefore, these systems do not mind about a natural face expression. However, facial expression including eyes are a key component and considered very important for human viewers.

Some information about the face can be lost beyond reconstructability (e.g. eye color). Other information (such as skin color) can be extrapolated from the visible skin. Furthermore, some algorithms need a specific face template to reconstruct with. For such cases it is convenient to have additional information encoded on/in the PET along side a privacy policy with finder granularity.

One of the most promising approaches is Lin et al. [18]. It provides convincing natural looking results on grayscale images. It does not need an exact reference face. Skin color can be extrapolated in an additional step from other visible skin parts. Moe et al. [19] focuses in his work just on the eye and mouth part, and is a good choice for morphing the reconstructed face onto tilted or turned away heads. Hwang et al. [20] offers good results on face images in natural environment and overcomes the limitations of their former work which needs a pixelwise mapping between the faces.

Limitations All discussed methods can not reconstruct facial expressions that have been destroyed. Also most algorithms assume frontal shots. Therefore, a straightening or a morphing algorithm needs to be employed to deal with turned away or tilted faces.

Some information about the face (e.g. eye color) should be encoded within the transitional PET. Additionally, if the original face was already partly otherwise occluded (e.g. a hand before the mouth), the algorithms might remove the hand in order to recreate the face. Such cases can be handled by focusing only on the eye part (in the case of Privacy Visor).

5.2 Detection of the Destructed Face

The face pattern is destroyed by the 1st generation PET albeit typically needed by the 2nd generation PET to attach and apply the privacy policy to a pictured person. Thus, the transitional PET decoder has to be given other ways to detect the face. A robust way is to include an additional visual marker to the PET. This marker should include a directional aspect, similar to augmented reality markers. This will allow for more realistic face reconstructions.

5.3 Policy Encoding

Encoding the policy can be done using any other 2nd generation picture PET. However, it is beneficial to include it directly onto the 1st generation PET. This way, it is highly probable that all parts of the PET will be visible in a single image. Thus, ensuring that all parts of the 1st and 2nd generation PET fit together and are interpreted as intended.

6 Overview of the Smart Privacy Visor

With the *Smart Privacy Visor* (SPV) concept we visualize how this transition technology can by applied to link the Privacy Visor (Figure 1d) [3] with the Picture Privacy Policy Framework (P3F) [7].

- The SPV is based on the latest Privacy Visor. The Privacy Visor in its current form consists of a pair of goggles with structured a white surface. The latter will become handy, when additional information needs to be encoded.
- A *face orientation marker* is included, disguised as a nose holding piece.
- The face orientation marker above doubles as *transition marker*. Thus, helping the transitional privacy image processor to detect the occluded face and its transitional PET properties.
- A P3F [7] policy is included either as colored dots into the frame (based on [21]) or directly onto the white surface of the Privacy Visor. The latter encoding is heavily inspired by 2D barcodes, such as QR, Aztec or MaxiCode. Special care must be taken, not to create a new visual property that facilitates identification or tracking of the person.
- Additional face reconstruction data is also stored in the 2D bardcode. However, we did not include data of the original face, as it would facilitate biometric identification and contradicts the privacy needs of users wearing such a PET. If necessary, a generic face template database can be used by the decoder with only the index to a specific template is included. This way, many people will share the same face template.

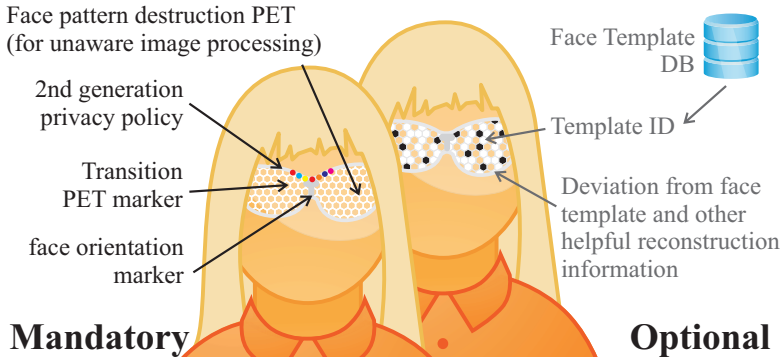


Fig. 5: Smart privacy visor as transition solution between 1st and further generations of picture PETs. Examples of encoding information on the Smart Privacy Visor: Left side based on Jimenez et al. [21]. Right side encoding using 2D barcode similar to Semacode, QR or Atzec code.

– If needed, deviations from the face template can be stored. This includes the color of the eyes.

7 Conclusion

The problem of unintentionally and involuntarily photographed and published individuals have been recognized by a number of publications in recent years. This is a problem not only of privacy aware citizens but sparks legal uncertainty among professional photographs, picture processors and users, and publishing houses. We identified there main classes of wearable picture-related Privacy Enhancing Technologies (PETs). As they need different prerequisites to operate and become effective they have unique time frames where they can be effective. The group of *face pattern destroying picture PETs* works against current face detection algorithms and can be used right away. However, they have different drawbacks and are likely to be superseded as soon as later generations of picture PETs become operational. In contrast to first generation picture PETs, the later systems do now show a general destructive behavior to the depicted faces. This upcoming transition is the main objective of our work: We described a novel method how to create transitional PETs that confirm to multiple generation systems and are able to revert the destructive effects of the first generation's methods facilitating face reconstruction algorithms.

We described first in general what the challenges of an transitional PET are and how to overcome them. Finally, we presented the *Smart Privacy Visor* which combines *Privacy Visor* and the *Picture Privacy Policy Framework*. This transitional PET have to be designed particular carefully as to not create new identifiable and linkable properties which contradict the goals of picture PETs in the first place.

Acknowledgment

This work is supported by the National Institute of Informatics' internship program, a *netidee* grant by the Internet Foundation Austria (IPA), and the *Comet K1* program of the Austrian Research Promotion Agency (FFG).

References

1. Harvey, A.: CV Dazzle (2010-2012) `http://cvdazzle.com/` and `http://ahprojects.com/projects/cv-dazzle`, accessed Nov 2nd 2014.
2. Yamada, T., Gohshi, S., Echizen, I.: Use of invisible noise signals to prevent privacy invasion through face recognition from camera images. In: Proceedings of the 20th ACM international conference on Multimedia. MM '12, ACM (2012) 1315–1316
3. Yamada, T., Gohshi, S., Echizen, I.: Privacy visor: Method for preventing face image detection by using differences in human and device sensitivity. In: Communications and Multimedia Security, Springer (2013) 152–161
4. Yamada, T., Gohshi, S., Echizen, I.: Privacy visor: Method based on light absorbing and reflecting properties for preventing face image detection. In: Systems, Man, and Cybernetics (SMC), 2013 IEEE International Conference on, IEEE (2013)
5. Patel, S.N., Summet, J.W., Truong, K.N.: Blindspot: Creating capture-resistant spaces. In: Protecting Privacy in Video Surveillance. Springer (2009) 185–201

6. Schiff, J., Meingast, M., Mulligan, D.K., Sastry, S., Goldberg, K.: Respectful cameras: Detecting visual markers in real-time to address privacy concerns. In: Protecting Privacy in Video Surveillance. Springer (2009) 65–89
7. Dabrowski, A., Weippl, E.R., Echizen, I.: Framework Based on Privacy Policy Hiding for Preventing Unauthorized Face Image Processing. In: Systems, Man, and Cybernetics (SMC), 2013 IEEE International Conference on, IEEE (2013)
8. Pallas, F., Ulbricht, M.R., Jaume-Palasí, L., Höppner, U.: Offlinetags: A Novel Privacy Approach to Online Photo Sharing. In: CHI '14 Extended Abstracts on Human Factors in Computing Systems, ACM (2014) 2179–2184
9. Barhm, M.S., Qwasmi, N., Qureshi, F.Z., El-Khatib, K.: Negotiating privacy preferences in video surveillance systems. In: Modern Approaches in Applied Intelligence. Springer (2011) 511–521
10. Henne, B., Szongott, C., Smith, M.: Snapme if you can: privacy threats of other peoples' geo-tagged media and what we can do about it. In: Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks, ACM (2013) 95–106
11. Brassil, J.: Using mobile communications to assert privacy from video surveillance. In: Parallel and Distributed Processing Symposium, 2005. Proceedings. 19th IEEE International, IEEE (2005) 8 ff.
12. Yus, R., Pappachan, P., Das, P.K., Mena, E., Joshi, A., Finin, T.: Demo: Faceblock: privacy-aware pictures for google glass. In: Proceedings of the 12th annual international conference on Mobile systems, applications, and services, ACM (2014)
13. Wickramasuriya, J., Datt, M., Mehrotra, S., Venkatasubramanian, N.: Privacy protecting data collection in media spaces. In: Proceedings of the 12th annual ACM international conference on Multimedia, ACM (2004) 48–55
14. Chinomi, K., Nitta, N., Ito, Y., Babaguchi, N.: Prisurv: Privacy protected video surveillance system using adaptive visual abstraction. In: Advances in Multimedia Modeling. Springer (2008) 144–154
15. Moon, H.M., Seo, C.H., Chung, Y., Pan, S.B.: Privacy protection technology in video surveillance system. In: Embedded and Multimedia Computing, EM-Com 2009. 4th International Conference on, IEEE (2009) 1–6
16. Ashok, A., Nguyen, V., Gruteser, M., Mandayam, N., Yuan, W., Dana, K.: Do Not Share! Invisible Light Beacons for Signaling Preferences to Privacy-Respecting Cameras. In: Proceedings of the 1st ACM MobiCom workshop on Visible light communication systems, ACM (2014) 39–44
17. Koster, M.: A Standard for Robot Exclusion `http://www.robotstxt.org/orig.html`, accessed July 15th 2015.
18. Lin, D., Tang, X.: Quality-driven face occlusion detection and recovery. In: Computer Vision and Pattern Recognition, 2007. CVPR'07, IEEE (2007) 1–7
19. Mo, Z., Lewis, J.P., Neumann, U.: Face inpainting with local linear representations. In: BMVC. (2004) 1–10
20. Hwang, B.W., Lee, S.W.: Reconstructing a whole face image from a partially damaged or occluded image by multiple matching. In: Advances in Biometrics. Springer (2007) 692–701
21. Jimenez, A.E., Dabrowski, A., Sonehara, N., Martinez, J.M.M., Echizen, I.: Tag detection for preventing unauthorized face image processing. In: Proceedings of the 13th International Workshop on Digital-Forensics and Watermarking (IWDW 2014), LNCS, Springer (October 2014)