HAL open science

Revocable Anonymisation in Video Surveillance: A "Digital Cloak of Invisibility"

Linus Feiten, Sebastian Sester, Christian Zimmermann, Sebastian Volkmann, Laura Wehle, Bernd Becker

To cite this version:

Linus Feiten, Sebastian Sester, Christian Zimmermann, Sebastian Volkmann, Laura Wehle, et al.. Revocable Anonymisation in Video Surveillance: A "Digital Cloak of Invisibility". 12th IFIP International Conference on Human Choice and Computers (HCC), Sep 2016, Salford, United Kingdom. pp.314-327, 10.1007/978-3-319-44805-3_25 . hal-01449444

HAL Id: hal-01449444

https://inria.hal.science/hal-01449444

Submitted on 30 Jan 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Revocable Anonymisation in Video Surveillance: a "Digital Cloak of Invisibility"

Linus Feiten, Sebastian Sester, Christian Zimmermann, Sebastian Volkmann, Laura Wehle, and Bernd Becker

University of Freiburg, Centre for Security and Society,
Bertoldstrasse 17, 79085 Freiburg, Germany
{feiten,sesters,wehle,becker}@informatik.uni-freiburg.de,zimmermann@iig.uni-freiburg.de,sebastian.volkmann@philosophie.uni-freiburg.de

Abstract. Video surveillance is an omnipresent phenomenon in today's metropolitan life. Mainly intended to solve crimes, to prevent them by realtime-monitoring or simply as a deterrent, video surveillance has also become interesting in economical contexts; e.g. to create customer profiles and analyse patterns of their shopping behaviour. The extensive use of video surveillance is challenged by legal claims and societal norms like not putting everybody under generalised suspicion or not recording people without their consent. In this work we propose a technological solution to balance the positive and negative effects of video surveillance. With automatic image recognition algorithms on the rise, we suggest to use that technology to not just automatically identify people but blacken their images. This blackening is done with a cryptographic procedure allowing to revoke it with an appropriate key. Many of the legal and ethical objections to video surveillance could thereby be accommodated. In commercial scenarios, the operator of a customer profiling program could offer enticements for voluntarily renouncing one's anonymity. Customers could e.g. wear a small infrared LED to signal their agreement to being tracked. After explaining the implementation details, this work outlines a multidisciplinary discussion incorporating an economic, ethical and legal viewpoint.

Keywords: video surveillance, privacy protection, anonymity, data security

1 Introduction

Today, life in urban areas is hardly imaginable without omnipresent video surveillance (VS). Screens showing the recorded images are installed in prominent locations to remind us that we are constantly being watched or even recorded. Ideally, this makes us feel more secure; but it might also reveal intimate details about our lives and make us change our behaviour in subtle yet profound ways, thereby threatening our rights to political liberty and personal self-determination.

VS can of course help to convict a criminal, preemptively detect imminent danger, or chase a fleeing suspect more effectively. It is also reported that the visible installation of cameras does in fact reduce crime in that respective area.

Thus, from a crime fighter's point of view there are clearly advantages of having as much VS as possible. With more installed cameras the monitoring and evaluation of recorded data becomes insurmountable for human operators. Therefore, efforts are made towards automatising the video analysis through computer algorithms – as it was e.g. the goal of the infamous EU project INDECT.

But not only crime fighters are interested in VS. In an emerging trend, VS has also come into the focus of commercial applications. Similar to internet users being tracked and analysed, people can be automatically identified and tracked on video recordings. Thus, e.g. a supermarket can track the paths customers take through the aisles, analyse where they stop or which advertisements catch their attention. The resulting data allows to optimise the arrangement of products or send customised promotions or discount offers based on the costumer's behaviour. Again, there are obvious advantages of VS in these scenarios: both for the shop owner (optimisation of products and advertising) and for the customers (individual discounts and a more seamless shopping experience).

However, in spite of legal norms governing the allowable use of VS, the public debate on its drawbacks or even threats to an open free society is not ceasing. A most prominent example is the so-called 'Big Brother Award', an annual ironic award by civil-rights activist to persons or organisations who have in their views greatly contributed to shifting society towards George Orwell's dystopia from '1984'. Among the German awardees, there were particularly VS related cases in the years 2000 (German Railways, surveillance of station platforms), 2004 (Lidl supermarkets, surveillance of employees) and 2013 (University of Paderborn, surveillance of lecture halls and computer labs).

In this work, we are discussing a possible reconciliation between these concerns about already present VS and its advantages for both crime fighting and economical endeavours. The *'Digital Cloak of Invisibility'* (DCI) is a generally applicable concept of anonymising personal information in vastly collected data [4] that is here applied to VS. This anonymisation, however, can be partially revoked if necessary. While there have been several studies about automatic privacy and intimacy preserving in VS and even some about revocable anonymisation, we first suggest an alternative method to achieve revocable anonymisation and – to best of our knowledge for the first time – present a scenario of how such a technology could be implemented in a modern society. In contrast to purely technical approaches, this work's main contribution is the multidisciplinary discussion of VS with revocable anonymisation within its societal (legal, economic and ethical) context.

Section 2 outlines the computer scientific details of the DCI, preparing the ground for a multidisciplinary discussion of the approach. Section 3 evaluates VS and the DCI from a legal perspective, exemplarily taking into account the German legislation. In order to provide a more holistic discussion of the societal implications of VS and the DCI, Section 4 discusses the DCI from an economical point of view, while Section 5 provides an ethical analysis of VS and how the respective concerns are met by the DCI. To preserve the scope of this paper, these viewpoints are kept very brief. The intend is to initiate a debate, whose main points and future directions are concluded in the final section.

2 Technological implementation

The problem of compromised privacy in VS has been addressed by several works; e.g. [10],[13],[17],[20],[24,25]. Most approaches automatically detect and irreversibly obfuscate privacy critical image regions like human silhouettes, faces or car licence plates. Some approaches like [7,8,9] have also suggested methods for revocable obfuscation. In contrast to these purely technical approaches, this work's main contribution is the multidisciplinary discussion of VS with revocable anonymisation within its societal (legal, economic and ethical) context. We therefore draft a rather simple yet efficient way for revocable image obfuscation; namely to XOR their pixel values with a pseudo-random cipher stream generated from a secret key seed. This scheme is sufficient to demonstrate the relevant concepts of embedding it into the societal context but could also be interchanged for any other possibly more sophisticated reversible obfuscation technique.

As more and more of the recorded video footage is going to be analysed automatically by pattern recognition algorithms, we propose to use the same algorithms to identify persons but *blacken* them before the footage is stored or viewed by a human. This blackening is done by a cryptographic method that allows to restore the original image with a key. This key is securely stored in the camera and by a publicly accepted *key keeper authority* (KKA). Whenever video footage is required to identify criminal suspects after an event, the crime fighter requests the required key from the KKA. For cases of imminent danger, a "break glass" functionality can immediately grant a key, leaving a log entry for the KKA to double-check. For commercial applications, the DCI allows shop owners to do their tracking of filmed customers – however, only of those who have agreed to being tracked, similar to the loyalty program 'Payback' where people agree to their shopping receipts being recorded and analysed in exchange for monetary compensation. ('Payback' was incidentally awarded a Big Brother Award in 2000.) People who agree to being tracked could signify their approval e.g. by wearing an inconspicuous tag on their clothes or by inserting a personal smartcard into their shopping cart.

As with classical VS, the recordings are made by a camera we assume to be digital, i.e. the video image is processed by digital circuits before the data is digitally transmitted out of the camera – an assumption that is valid for many VS cameras today and will in the future be true for all VS. The DCI extends such camera with additional internal circuitry that performs a certain post-processing on the video data before it leaves the camera's hardware. The workflow is depicted in Figure 1.

First, an image recognition algorithm identifies all persons in each video frame. The perfectly reliable implementation of such algorithms is nowadays still in its beginning ([3],[6],[11],[28]) but most certainly the future will see them running reliably on embedded systems like those of digital cameras. Each DCI-enhanced camera has a unique cryptographic key securely embedded in its hardware, called *Camera Master-Key* (CMK). For each video frame and image region showing a person, an individual *Sub-Key* (SK) is created by feeding the CMK with frame number and region coordinates to a *hash function* [26]. Strong hash functions have the property that the input cannot be derived from the output.

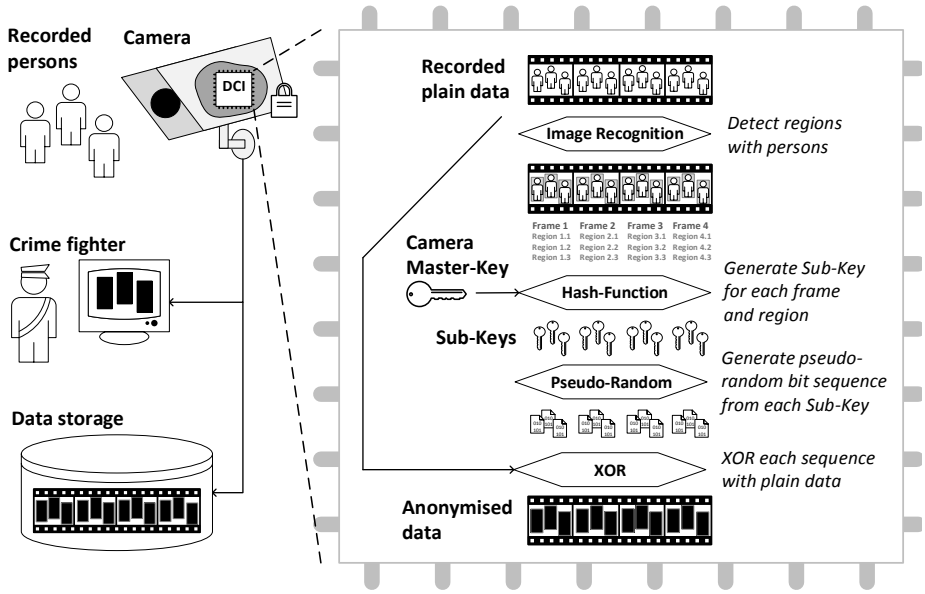

Fig. 1. The schematic concept of a DCI camera system.

Thus, it is not possible to derive the CMK from the SK – even if the used frame number and region coordinates are known.

The SKs are used to generate a pseudo-random cipher-stream of bits that is XORed with the pixel data of the corresponding region in the original video frame. In the resulting video, this region appears obscured (in fact the pixels have random colours). The meaning of pseudo-random is that the generated bits look random, but the sequence solely depends on the respective SK, such that it can always be reproduced. The XOR function ($\oplus$) is reversible:

$$data \oplus cipherStream(SK) = encryptedData$$

$$encryptedData \oplus cipherStream(SK) = data$$

Thus, the blackening of a region in a frame can be undone, when the respective SK is known. This is applied in the DCI deanonymisation scheme shown in 2. If a crime is recorded, the crime fighter makes a request to the KKA which verifies its legitimacy and then grants the SKs for the requested frames and image regions. Only the suspect persons in a recording can be deanonymised while all others remain anonymous.

To cater for cases of imminent danger, a “break glass” functionality is implemented such that a sequence of SKs can be requested remotely (e.g. via internet) and is automatically granted. This, however, leaves a log entry with the KKA such that the request’s legitimacy and whether the “break glass” was justified can be verified afterwards.

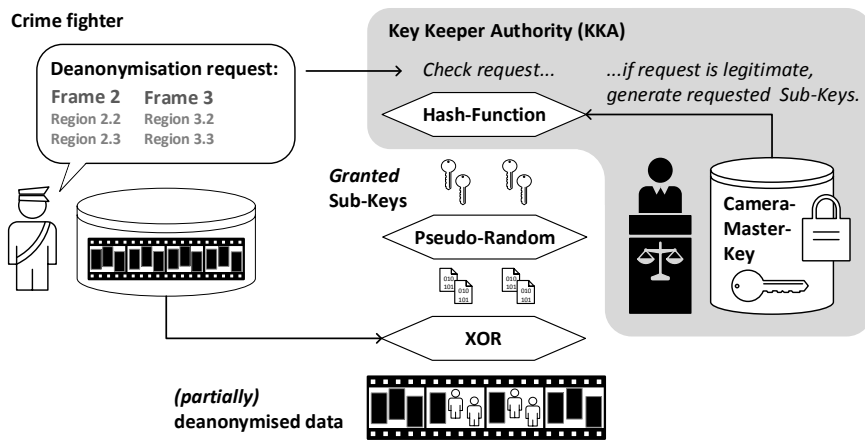

Fig. 2. Deanonymisation is only possible with the SKs granted by the KKA.

In a first proof of concept, we implemented a DCI camera as an *opt-out* system instead of *opt-in*. I.e. instead of anonymising everybody by default except those who opt-in, nobody is anonymised except those who opt-out (conceptually similar to [24]). This was done to firstly abstract from the person-identifying image recognition. We designed an infrared LED beacon that is picked up by the camera to subsequently anonymise the region around this beacon. Figure 3 shows the practical results. The anonymisation is done with the cryptographic scheme as described above. With sufficiently reliable person-identifying algorithms, the system can easily be transformed into the DCI opt-in variant.

Fig. 3. A first proof-of-concept implementation of the DCI as opt-out: only regions surrounding a detected infrared beacon are anonymised.

3 Legal considerations

In 1995, the European Union issued the Data Protection Directive (95/46/EC) to be implemented by all member states. In this section, we exemplarily focus on the German implementation of the directive in its Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG). The legal basis regulating the use of VS (§ 6b BDSG [1]) only allows it under specific circumstances. The VS has to be both *sufficient* to reach the intended purpose and *necessary*; i.e. there has to be no less severe economically reasonable alternative [12, paragraph 236]. Furthermore, a weighing of interests must be fulfilled between the intended VS purpose and the constitutional personal rights of the affected (Article 2 paragraph 1 of the Basic Law for Germany), i.e. in particular the right to one's own image and the right to informational self-determination [5, paragraph 22].

The *sufficiency* of VS is mostly given, insofar as it is assumed to fulfil its typical purposes: crime prevention, detection and deterrence. But also the *necessity* is generally easy to prove with the argument that high personnel costs are hardly an economically reasonable alternative to the comparably cheap VS equipment [5, paragraph 21]. The weighing of interests is mostly decided in favour of the intended purpose, as § 6b BDSG allows VS to be used for exercising one's right to domestic authority, or – even more generally – to exercise any justified interest for a concretely defined purpose; and justifications – like the state's obligation to avert danger and prosecute crime or the individual's interest in protection of one's property – mostly outweigh the mentioned personal rights of the VS affected, as long as the VS is not done covertly but clearly signified. Furthermore, recordings must not be stored longer than required to fulfil the respective purpose, which of course can allow for rather long time spans depending on the purpose interpretation.

Evaluating the *necessity* of classical VS versus the DCI, it can be asserted that the DCI is in fact a less severe alternative. As all people are anonymised by default, there is no infringement of personal rights any more. These benefits should outweigh the slightly higher costs in most cases, such that the DCI can also be considered an economically reasonable alternative.

Whether it is also *sufficient* in the same way as classical VS requires a more thorough analysis. The foremost purpose of VS is to identify recorded suspects in hindsight, which is definitely also provided by the DCI. If recordings are to be analysed in a typically already protracted criminal proceeding, the relatively short delay of requesting the SKs from the KKA does no harm. For emergencies, there is the "break glass" functionality to immediately get a set of SKs. Another purpose of VS is the deterrent effect, which is also catered for by the DCI. Because people will be aware that they will be deanonymised if the crime fighter convinces the KKA of the crime having taken place. This will in most cases be possible by pointing out the respective scenes in the anonymised recordings, because most suspicious actions are still recognisable, even if the "protagonists" are obscured. This is also the reason why DCI-enhanced VS is just as suitable for real-time monitoring. Turmoils or robberies, for example, show typical patterns of movement that are easily spotted irrespective of whether the persons are obscured or not. It can thus be concluded that the *sufficiency* is fulfilled.

In economical scenarios, where customers renounce their anonymisation in a loyalty program (cf. Section 4), the DCI is legally rather unproblematic. The operator simply has to comply with § 6b BDSG by signifying the use of VS and to let the participating customers sign his general terms and conditions (cf. § 4 and § 28 BDSG).

Of course, this exemplary discussion of the German legal context is not exhaustive and other legal contexts could be included. Furthermore, technical concepts like the DCI have hardly been taken into account in the legal practice. Thus, in addition to the following economic consideration, Section 5 extends the limited normative discussion presented above by including an ethical analysis. This will allow us to look more broadly at normative issues and conflicts introduced by VS and how the DCI can address these in a constructive way.

4 Economic Applications

DCI systems can not only be utilised for protecting individuals' privacy in the context of VS-based crime prevention and detection. They also allow for conducting economically motivated video surveillance in a privacy-aware manner. In the following, the potential of the here presented system in the context of customer analysis for marketing in brick and mortar stores is discussed.

Store owners have long used video surveillance systems not only to deter shoplifters but also for being able to present evidence in case of incidents within their premises. However, video surveillance systems are also suited to precisely track customers' movement and even their direction of view [18,19]. This allows shop owners to gain valuable insights that can be used for marketing, e.g. for shop design or advertising campaigns. In Germany, however, customers' high privacy concerns are an impediment to the adoption and usage of such analysis methods. The here presented DCI system has the potential of addressing these concerns on the one hand and to guarantee that only the movements and behaviour of customers who have consented are tracked, on the other hand.

The DCI system can be used analogously and complementary to the currently popular loyalty cards in order to restrict tracking and behavioural analysis within the store to customers who have consented on the one hand, and, on the other hand, to reduce the privacy concerns of customers who have not consented. Two options to harness this potential exist. In its current state of implementation, the presented DCI system can be utilised as an easy opt-out mechanism. Through wearing a respective signal emitter, e.g. on their clothes or on their shopping cart, customers can opt-out of movement tracking and behavioural analysis. However, this application would be in stark contrast to the "privacy-by-design" requirement as laid down in the current draft of the new European General Data Protection Regulation [14, Art. 23]. Still, the DCI can also serve as an opt-in mechanism. Customers who consent to being tracked within the store can signal this through signal emitters on their clothes or shopping carts. For example, infrared LEDs could be used in this scenario, emitting light signals that correspond to a customer account or profile. This would also allow for combing the DCI with existing loyalty programs. In that scenario, the VS system

would have to encrypt the whole video by default except for regions in which a respective signal is detected. A problem to be solved in the commercial scenario is the selection of an appropriate KKA. Further, the presented system has to be extended in order to prevent "bycatch". In case two customers, one who consented to tracking and analysis and one who did not, are standing close to each other in the store, the will of the customer who did not consent should be prioritised and both customers are anonymised.

5 Ethical impact assessment

Due to the complex nature of both society and technology development, an ethical impact assessment should not be considered an accurate prediction of the future. Rather, it can be seen as a projection of intended and unintended consequences of technology use and of the potential moral risks and chances. Especially with regard to unintended consequences (side effects) of using new technologies, legal frameworks often lag behind and do not address emerging conflicts adequately. Ethical impact assessment then sketches plausible scenarios and outcomes that can be used as a normative basis for deciding how to deal with technological change in society. In many cases, as done here with regard to the DCI, this normative basis can then be used constructively in the development process. In this way, at least some of the foreseeable moral risks – even if they are not yet fully covered by the legal framework – can be addressed by technological means [22].[1]

If we take a closer look at the unintended ethical impact of implementing VS technologies in public places, two argumentative perspectives can be differentiated: (1) the unintended impact can affect specifiable individuals, especially with regard to their fundamental rights and liberties; or (2) the unintended impact can affect the character of a society as a whole, especially by contributing to developments that make it more restrictive. The latter perspective becomes especially important in cases where the impact for most specifiable individuals is comparably small or mostly indirect, but where, in sum, we can still foresee a considerable impact on the openness of society. Examples for this is the subtle but constant expansion of security technologies over a longer period of time (sometimes called the 'boiling frog argument' [27]) or the ex post expansion of the purpose of data collection ('mission creep argument' [21]).

In the remainder of this section, we present a brief assessment of the ethical impact of VS with and without the use of the DCI. This is done by means of four metaphors [16] that are commonly invoked by critics in the relevant public and scientific debates in Germany.[2] Regarding the ethical impact on specifiable individuals, we first look at the commonly perceived risk that the private lives of

[1] Of course, not all moral risks can be addressed technologically and every technological "fix" may introduce new unintended consequences. Therefore, constructive ethical impact assessment should rather be seen as a continuous process of reflection than as providing a static set of design requirements.

[2] Although we focus on metaphors from the German speaking debate, the terms translate well and are just as informative for English speaking debates.

customers or citizens become "transparent" to commercial and governmental actors (*gläserner Kunde/Bürger*). Afterwards we discuss the fear that persons under VS are subject to what is called a "generalised suspicion" (*Generalverdacht*). Regarding the ethical impact on society as a whole, we look at the metaphors of an "Orwellian" and a "Kafkaesque surveillance society".

5.1 Individual centric perspective

In the discussion about spatially limited VS in publicly accessible places, the metaphor of the transparent customer predominantly denotes the fear that commercial actors may collect and process data about their customers to an extent that they can infer facts about their wishes, intentions and living situations. Such information often includes private or even intimate facts that are widely considered to be worthy of protection based on cultural norms of modesty (e.g. regarding sexuality or illness) or based on the societal fear that some individuals may be affected disproportionately (e.g. due to their financial or social situation). Furthermore, since intimacy depends on *selective* sharing of information, the control over information about oneself has been recognised as a necessary precondition to establish relationships with varying levels of intimacy as well as for the development of our personality free from the impingement of others [15]. In contrast to this, the metaphor of the transparent citizen predominantly denotes the fear of far-reaching data collection and processing on behalf of state actors. Here, the reason for considering certain information private and worthy of protection is founded additionally in the fear of governmental overreach and an overly powerful state. In democracies, therefore, state sponsored VS must always be viewed in relation to rights and liberties that defend the individual against the state. In comparison to commercial actors, state actors are therefore usually subject to stricter checks of proportionality and more often require the implicit or explicit consent of the affected individuals.

In both cases, however, such privacy intrusions are often considered justifiable (especially in a legal sense) if they allow the protection of other societal values – for example if there is the suspicion of criminal activities. Here, the metaphor of the generalised suspicion expresses the fear that security measures such as VS may be used indiscriminately so that *all* individuals may be subject to privacy intrusions on the basis that *some few* individuals could be said to have criminal intentions.

In classic forms of VS, individuals can generally be identified either manually or automatically by making use of biometric facial recognition or other optical criteria. In addition to that, the tracking of their movements throughout the area under surveillance can allow to establish buying patterns, to infer personal intentions or to reveal intimate aspects of their living situations. How much time did this customer spend in front of the shelves with the condoms and how often does she come to buy liquor? Does this person commonly use the public transport system during working hours? How long does that man talk to the preacher in the public square, how long to the people from the election campaign? Especially techniques of long-term storage and automated analysis of video data can present a severe infringement of individual privacy and the free

development of personality that goes far beyond what people have to assume anyway when they move in public places.

By obscuring the information that allows the identification of individuals in the video images, this moral risk can be mitigated effectively as the recorded data cannot be directly related to specific individuals. Depending on the implementation of the KKA, such an intrusion is only allowed in cases where the reason for it is checked and considered legitimate by an independent instance – for example to collect evidence in case of shop lifting or assault. Furthermore, even in such cases, only specific pieces of information can be revealed, such as data relating to concrete individuals during a specific time frame. At the same time, the intended benefit of the VS – e.g. police officers watching a public area to react quickly in case of assaults or a shop detective watching the customers to spot shop lifters – can still be achieved. Both scenarios show that the usage of a DCI system can protect the privacy and intimacy of customers or citizens much better than classic forms of VS. Furthermore, they allow restricting legitimate intrusions to the necessary information.

5.2 Society centric perspective

The term surveillance society is used to express concerns about the prevalence of surveillance measures of commercial or state actors throughout society. In the context of VS, the term does therefore not refer to singular, isolated instances or strictly limited locations, but rather to the gradual proliferation of this measure and the threat that those systems could be networked bit by bit and the recorded information merged to a large pool of surveillance data. In this context, the metaphor of the Orwellian surveillance society denotes the concern that the proliferation of surveillance measures may lead to a situation in which we are almost constantly monitored and where we can never be sure how our behaviour will be interpreted or which negative consequences might ensue later on. From a democratic point of view, this implies the risk that the realisation of some of our rights and liberties may fall victim to a form of self-control – for example because we fear a more negative credit rating or being classified as a high risk airline passenger. This can be seen as a pressure towards a certain standard of normalcy that limits the open character of our society to a considerable extent.

In addition to that, the metaphor of the Kafkaesque surveillance society expresses the fear that we may loose the de facto possibility of achieving an effective remedy in case we suffer illegitimate negative consequences. This is especially relevant in cases where it is highly opaque why the relevant decisions were taken, based on which information and on which criteria and how those decisions can be disputed. With regard to VS measures, this risk becomes material especially in those cases where recorded data is handed over or even sold to third parties without the consent of affected persons, since this would facilitate the consolidation and misuse of data from different sources – for example in order to allow pattern recognition for the detection of potential criminals or insurance risks.

In classic forms of VS, it is very difficult to effectively limit the circulation and processing of the recorded data. Even in cases where signs inform customers

or citizens explicitly about the VS, it is almost impossible to foresee what information can be inferred from the recorded data and how it could be used in the future. Some of these risks can be mitigated to a certain extent when surveillance actors promise to restrict themselves in the use of such data – but it is unclear what would be the incentive for commercial actors to do so and how misuse could be sanctioned effectively. The use of a DCI system by commercial or governmental actors, on the other hand, allows the use of the KKA as an independent party to effectively mitigate the risk of circulation, consolidation from different sources and misuse of the recorded data. This is especially true if only those pieces of data are revealed that are strictly necessary for a certain legitimate purpose. Furthermore, for commercial surveillance actors, it could be an incentive for the use of a DCI system if they can advertise their use of higher standards of protection of their customers' privacy. For both the commercial and governmental case, we can thus conclude that a DCI system allows to also effectively mitigate the society centred ethical risks of circulation of surveillance data, of data consolidation from different sources and of misuse of that data.

6 Discussion and Conclusion

The advantages of a DCI-enhanced VS system over the kind of VS that is already massively in use today has been demonstrated in each perspective of our multidisciplinary discussion. Still, there might be remaining criticisms towards DCI that shall be addressed in the following.

A concern raised from someone generally opposing VS could be, that a DCI technology would merely be a fig leaf for VS; leading to a higher rate of social acceptance followed by an implementation of even more VS systems. That concern would be justified if VS today would in fact be used very sparsely. Reality, however, shows that we are already living in a society where VS is implemented on a large scale, mostly accepted or not pondered over by large parts of the populace. Replacing it with DCI systems will be given just as little thought by those, but people concerned about VS today will experience a real improvement.

Another such concern could be about the DCI security. The whole DCI system relies on the CMK's secure storage both in the respective camera and in the KKA's central storage. If the CMK is obtained e.g. by a hacker attack, all recordings made with the respective camera could be deanonymised. As a precaution, it is therefore recommendable to keep the same strict constraints of how long recordings may be stored that are in place today for classical VS. Then, even if the DCI security should get compromised, it would only be as "bad" as it is right now without DCI. To keep a CMK save in the hardware of a camera there is a manifold of techniques from the field of hardware security and trusted hardware. e.g. *tamper-sensing Meshes* [2] or *Physically Unclonable Functions* (PUFs) [23]. Equivalently, the KKA's storage has to be secured with state of the art security measures.

Another question is: "Who is the KKA?" The trust of the populace in the KKA's integrity is essential. Thus, one could consider a democratic board unsuspicious of collaborating with the respective camera operator. We presume that

among the civil-rights activist now fighting against VS many would volunteer to be part of a KKA and that they would be trusted; particularly by those sceptical of VS. Another possibility could be a judge or ombudsman to decide about when a key request is granted. In any case, transparency and accountability of the KKA's decisions and procedures are paramount for the creation of trust.

One also has to be aware, that DCI-enhanced VS does not provide perfect anonymity. An obscured person might still be identified by a diligent analyst e.g. by the fact that she was walking a dog or because he was – although anonymised – observed leaving his residency. With an extension of the DCI algorithm these sources of identification could be further hampered, but one should not be illusionary about the limits of anonymisation.

A last concern could come from advocates of classical VS; namely that a DCI is more expensive than classical VS. This is of course true. The extra hardware in the cameras and the administrative efforts to regulate the exchange of requests and keys between the crime fighting instances and the KKA does not come for free. The question we have to ask ourselves as a society is, whether a decrease of intrusion into our privacy and intimacy as well a decrease of infringements of our civil liberties would be worth that extra cost.

References

1. Gesetzentwurf Bundesregierung Drucksache 461/00 (18th August 2000), `http://dipbt.bundestag.de/doc/brd/2000/D461+00.pdf`
2. Anderson, R., Bond, M., Clulow, J., Skorobogatov, S.: Cryptographic processors - a survey. Proceedings of the IEEE 94(2), 357–369 (Feb 2006)
3. Andriluka, M., Roth, S., Schiele, B.: Pictorial structures revisited: People detection and articulated pose estimation. In: Essa, I., Kang, S.B., Pollefeys, M. (eds.) Proceedings of Computer Vision and Pattern Recognition (CVPR). pp. 1014–1021. IEEE (2009)
4. Becker, B., Müller, G., Polian, I.: Digital tarnkappe: Stealth technology for the internet of things. In: Gander, H.H., Perron, W., Poscher, R., Riescher, G., Würtenberger, T. (eds.) Resilienz in der offenen Gesellschaft. Nomos (2012)
5. Becker, T.: Verlag Dr. Otto Schmidt, 1 edn. (2013)
6. Benenson, R., Mathias, M., Timofte, R., Gool, L.V.: Pedestrian detection at 100 frames per second. In: Belongie, S., Blake, A., Luo, J., Yuille, A. (eds.) Proceedings of Computer Vision and Pattern Recognition (CVPR). pp. 2903–2910. IEEE (2012)
7. Carrillo, P., Kalva, H., Magliveras, S.: Compression independent reversible encryption for privacy in video surveillance. EURASIP J. Inf. Secur. 2009, 5:1–5:13 (Jan 2009)
8. Cheung, S.C., Venkatesh, M., Paruchuri, J., Zhao, J., Nguyen, T.: Protecting and Managing Privacy Information in Video Surveillance Systems, pp. 11–33. Springer London, London (2009), `http://dx.doi.org/10.1007/978-1-84882-301-3_2`
9. Cichowski, J., Czyżewski, A., Kostek, B.: Visual Data Encryption for Privacy Enhancement in Surveillance Systems, pp. 13–24. Springer International Publishing (2013)
10. Cucchiara, R., Prati, A., Vezzani, R.: A system for automatic face obscuration for privacy purposes. Pattern Recognition Letters 27(15), 1809 – 1815 (2006), Vision for Crime Detection and Prevention

11. Dalal, N., Triggs, B.: Histograms of oriented gradients for human detection. In: Schmid, C., Soatto, S., Tomasi, C. (eds.) Proceedings of Computer Vision and Pattern Recognition (CVPR). pp. 886–893. IEEE (2005)
12. Detterbeck, S.: Allgemeines Verwaltungsrecht. Verlag C. H. Beck, 8 edn. (2010)
13. Dufaux, F., Ebrahimi, T.: Scrambling for video surveillance with privacy. In: Schmid, C., Soatto, S., Tomasi, C. (eds.) Proceedings of Computer Vision and Pattern Recognition (CVPR), Workshop Privacy Research in Vision (PRIV). pp. 160–160 (June 2006)
14. European Commission: Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Procedure 2012/0010/COD (2012), `http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf`
15. Fried, C.: An Anatomy of Values. Harvard University Press (1970)
16. Grin, J., Grunwald, A. (eds.): Vision assessment: shaping technology in 21st century society towards a repertoire for technology assessment. Springer (2000)
17. Huber, M., Müller-Quade, J., Nilges, T., Thal, C.: A provably privacy preserving video surveillance architecture for an assisted living community. In: 44. Jahrestagung der Gesellschaft für Informatik, Informatik 2014, Big Data - Komplexität meistern, 22.-26. September 2014 in Stuttgart, Deutschland. pp. 563–574 (2014)
18. Leykin, A., Hammoud, R.: Real-time estimation of human attention field in LWIR and color surveillance videos. In: Proceedings of Workshop on Object Tracking and Classification Beyond the Visible Spectrum (OTCBVS). pp. 1–6. IEEE (2008)
19. Liu, X., Krahnstoever, N., Yu, T., Tu, P.: What are customers looking at? In: Macq, B. (ed.) Proceedings of Advanced Video and Signal based Surveillance (AVSS). pp. 405–410. IEEE (2007)
20. Padilla-Lopez, J.R., Chaaraoui, A.A., Florez-Revuelta, F.: Visual privacy protection methods: A survey. Expert Systems with Applications 42(9), 4177 – 4195 (2015)
21. Pegarkov, D.D.: National Security Issues. Nova Publishers (Jan 2006)
22. Petermann, T.: Technikfolgen-Abschätzung – Konstituierung und Ausdifferenzierung eines Leitbilds. In: Bröchler, S., Simonis, G., Sundermann, K. (eds.) Handbuch Technikfolgenabschätzung, pp. 17–49. Edition Sigma (1999)
23. Ruhrmair, U., Devadas, S., Koushanfar, F.: Security based on physical unclonability and disorder. In: Tehranipoor, M., Wang, C. (eds.) Introduction to Hardware Security and Trust, chap. 4, pp. 65–102. Springer (2011)
24. Schiff, J., Meingast, M., Mulligan, D.K., Sastry, S., Goldberg, K.: Respectful cameras: detecting visual markers in real-time to address privacy concerns. In: Henderson, T.C. (ed.) Proceedings of Intelligent Robots and Systems. pp. 971–978 (Oct 2007)
25. Senior, A., Pankanti, S., Hampapur, A., Brown, L., Tian, Y.L., Ekin, A., Connell, J., Shu, C.F., Lu, M.: Enabling video privacy through computer vision. IEEE Security Privacy 3(3), 50–57 (May 2005)
26. Shi, Z., Ma, C., Cote, J., Wang, B.: Hardware implementation of hash functions. In: Tehranipoor, M., Wang, C. (eds.) Introduction to Hardware Security and Trust, chap. 2, pp. 27–50. Springer (2011)
27. Trojanow, I., Zeh, J.: Angriff auf die Freiheit: Sicherheitswahn, Überwachungsstaat und der Abbau bürgerlicher Rechte. Hanser (2009)
28. Walk, S., Schindler, K., Schiele, B.: Disparity statistics for pedestrian detection: Combining appearance, motion and stereo. In: Daniilidis, K., Maragos, P., Paragios, N. (eds.) Proceedings of European Conference on Computer Vision (ECCV). pp. 182–195. IEEE (2010)