Marion Koelle, Yvonne Brück, Vanessa Cobus, Wilko Heuten, Susanne Boll

# Respektvolle tragbare Kameras?

## Technische Gestaltung einer sozialakzeptablen Nutzung von Datenbrillen und Smart Cams


**Marion Koelle**

Wissenschaftliche Mitarbeiterin an der Carl von Ossietzky Universität Oldenburg, befasst sich seit 2009 mit Themen im Bereich der Augmented Reality (AR) und forscht derzeit zur sozialen Akzeptanz von AR und anderen kamera-basierten Anwendungen.
E-Mail: marion.koelle@uni-oldenburg.de

**Yvonne Brück**

Studentische Mitarbeiterin im BMBF-Projekt „ChaRiSma“, strebt derzeit den Abschluss ihres Studiums der Wirtschaftsinformatik in Oldenburg an.
E-Mail: yvonne.caroline.brueck@uni-oldenburg.de

**Vanessa Cobus**

Wissenschaftliche Mitarbeiterin am OFFIS – Institut für Informatik im BMBF-Projekt „ChaRiSma“ tätig.

E-Mail: vanessa.cobus@offis.de

**Dr. Wilko Heuten**

Leiter der Gruppe „Interaktive Systeme“ am OFFIS – Institut für Informatik in Oldenburg.

E-Mail: wilko.heuten@offis.de

**Prof. Dr. Susanne Boll**

Professorin an der Carl von Ossietzky Universität Oldenburg (Abteilung Medieninformatik und Multimediasysteme) und wissenschaftliche Leiterin des BMBF-Projekts „ChaRiSma“.
E-Mail: susanne.boll@uni-oldenburg.de


Der Bekanntheitsgrad tragbarer Geräte mit fest integrierter Kamera, wie etwa die Datenbrille *Google Glass* oder die Life Logging Kamera *Narrative Clip*, nimmt – nicht zuletzt durch die verstärkte Medienberichterstattung – immer mehr zu. Aber auch, wenn von diesen Geräten eine starke technische Faszination ausgeht, so werden sie doch häufig als sozial nicht akzeptabel kritisiert. Insbesondere die Anwesenheit einer – potentiell aufnehmenden – Kamera stellt eine Bedrohung für die Privatsphäre dar. Auch wenn das Tragen eines deaktivierten Gerätes faktisch keine unmittelbare Verletzung der Privatsphäre darstellt, so wird dessen Präsenz von Umstehenden als Eingriff in ihre Privatsphäre wahrgenommen. Unabhängig von rechtlichen Rahmenbedingungen wird bereits dadurch eine praktische Nutzung der Geräte im sozialen Umfeld unmöglich. In diesem Artikel stellen wir konkrete Schlüsselfragen vor, die beantwortet werden müssen, um eine sozialakzeptable Nutzung von Datenbrillen und anderen intelligenten Kamerageräten (Smart Cams) zu ermöglichen. Ziel ist es dabei, eine Nutzung zu ermöglichen, die respektvoll mit den Bedenken der Personen in der direkten Umgebung des Gerätenutzers umgeht und somit zu einer erhöhten Transparenz bezüglich Nutzung und Aufzeichnung von Kamerabildern beiträgt. Wir begründen diese Herangehensweise mit Erkenntnissen aus Nutzerstudien, die Faktoren der Akzeptanz bzw. Nichtakzeptanz von Datenbrillen genauer beleuchten. Dies erlaubt es unserer Forschung, eine Brücke zwischen technischer Innovation und einer sozialakzeptablen Nutzung von Datenbrillen und Smart Cams in der sozialen Interaktion im täglichen Leben zu schlagen.

## 1 Soziale Akzeptanz am Körper getragener Kameras

Am Körper getragene Life Logging Geräte mit fest verbauten Kameras – bekannte Varianten sind die Datenbrille Google Glass oder der Narrative Clip (eine „intelligente" Life Logging Kamera, oder Smart Cam) – haben bei ihrem Markteintritt starke Kritik und kontroverse Diskussionen hervorgerufen. Zentraler Kritikpunkt ist deren Fähigkeit, Menschen in der Umgebung unbemerkt per Bild und Video aufzuzeichnen – eine Bedrohung für die Privatsphäre der Umstehenden.

Zusätzlich führt die Miniaturisierung von Gerät und Kamera dazu, dass die Geräte unscheinbarer werden und unauffällig – meist unerkannt – getragen werden können (vgl. Abbildung 1). Das Wissen, dass „flüchtige Momente" potentiell immer und überall auf Video festgehalten werden könnten, ist für die meisten Menschen unangenehm, insbesondere, wenn dies ohne deren Kenntnis oder Zustimmung passiert.[1] Meist ist es den Umstehenden zudem völlig unklar, was das jeweilige Gerät technisch kann und auf welche Art und in welchem Umfang aufgezeichnet werden kann. Doch auch allein das Tragen der Kamera wird bereits als Beeinträchtigung der Privatsphäre betrachtet, auch wenn sie gerade gar nicht aufzeichnet.[2] Die Beschwerden über den "kodak fiend" (zu Deutsch: „Kodak Unhold") im Jahr 1890 – dem Jahr nach dem Erscheinen der ersten Kodak Kamera für private Nutzung – zeigt, dass die Bedenken von Umstehenden gegenüber fotografischen Aufnahmen schon nahezu so alt sind wie die Fotografie selbst[3]. Denning et al.[4] weisen jedoch darauf hin, dass die Bedenken gegenüber den aktuellen Geräten eine ganz neue Qualität besitzen, da diese unauffälliger zu benutzen sind als herkömmliche, in der Hand gehaltene Kameras. Die mangelnde Verbreitung bei gleichzeitig starker Medienpräsenz unterscheidet sie ebenfalls von herkömmlichen Geräten.

**Abbildung 1 | Eine unauffällig am Tragegurt eines Rucksacks befestigte Smart Cam ist oft erst bei genauem Hinsehen erkennbar.**


Life Logging-Technologien bergen ein enormes Potential für eine Vielzahl von Anwendungen,[5] die sich positiv auf verschiedene Teile unserer Gesellschaft auswirken könnten – sofern deren sozialakzeptable Nutzung möglich gemacht werden kann. Derzeit bewirkt die starke soziale Ablehnung der Technologie, dass die Trägerinnen und Träger sich in einem Spannungsfeld zwischen dem Nichtverwenden der Technologie – einer potentiellen Einschränkung ihres persönlichen Rechts auf freie Entfaltung – und negativen Konsequenzen im sozialen Umfeld, von Kritik bis hin zum Ausschluss, befinden.

Es ist daher notwendig, die mit der Nutzung verbundenen Bedenken und Ängste besser zu verstehen, um passende Lösungen der Technikgestaltung zu entwickeln. Die Allgegenwärtigkeit der tragbaren Kameras stellt dabei neue und bislang wenig untersuchte Herausforderungen an das Design sozialakzeptabler Technologie. Dieser Artikel fasst aktuelle Erkenntnisse aus diesem Bereich zusammen und gibt erste Einblicke in das partizipative Design der sozialakzeptablen Nutzung von Smart Cams und anderer, am Körper getragener Kameras. Dafür relevante Schlüsselfragen werden vorgestellt und Technologieoptionen anhand des aktuellen Stands der Technik verdeutlicht.

## 2 Einflussfaktoren auf die Rezeption von Datenbrillen

Die gesellschaftliche Akzeptanz neuer Technologien ist grundlegende Voraussetzung für deren erfolgreichen Einsatz sowie für ein konfliktfreies Miteinander von Technologienutzern und Anderen in ihrem sozialen Umfeld. Trotz vielversprechender Anwendungsfälle sind Datenbrillen (engl.: data glasses) auch mehr als vier Jahre nach ihrem Bekanntwerden in der breiten Öffentlichkeit[6] noch kaum sozial akzeptiert.

In einer Reihe von Forschungsarbeiten wurden die Gründe für diesen Mangel an sozialer Akzeptanz sowie Voraussetzungen einer erfolgreichen Integration in den Alltag der sogenannten Disruption[7] untersucht.

In einer über drei Jahre hinweg durchgeführten Benutzerstudie mit 118 Teilnehmern wurden über 64 Einsatzszenarien von Datenbrillen jeweils aus der Perspektive des Nutzers (Perspektive der 1. Person) und einer weiteren, in dem jeweiligen Szenario involvierten Person (Perspektive der 2. Person) evaluiert. Dafür wurden den Probanden skizzenhaft dargestellte Szenarien (z. B. „geschäftliche Besprechung", „zufälliger Gegenüber im öffentlichen Nahverkehr" oder „private Unterhaltung") gezeigt, die sie anschließend anhand eines semantischen Differentials bewerteten. Bei der Auswertung der Befragung wurden Unterschiede in

1 Bohn/Coroamă/Langheinrich/Mattern/ Rohs, "Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing," in: Weber/Rabaey/Aarts (Hrsg.), *Ambient Intelligence*, Berlin 2005, S. 5–29.

2 *Koelle/Kranz/Möller*, "Don't Look at Me That Way!: Understanding User Attitudes Towards Data Glasses Usage", in: *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*, New York 2015, S. 362–372.

3 "The Kodak Fiend" Hawaiian Gazette (Honolulu, Hawaii), December 9, 1890, Chronicling America Collection, Library of Congress.

4 *Denning/Dehlawi/Kohno*, "In situ with Bystanders of Augmented Reality Glasses: Perspectives on Recording and Privacy-mediating Technologies", in: *Proceedings of the 32rd Annual ACM Conference on Human Factors in Computing Systems*, New York 2014, S. 2377–2386.

5 Ein Beispiel für ein vielversprechendes Einsatzszenario von Life Loggingtechnologien ist zur Unterstützung der Erinnerungsfähigkeit, z. B. bei Demenz, wie sie im FET Projekt Recall untersucht wird, http://recall-fet.eu/ (Stand 10.01.2017).

6 Google's Projekt Glass, später bekannt als Google Glass wurde erstmals am 4.4.2012 auf der Plattform Google+ der Öffentlichkeit vorgestellt, https://plus.google.com/+GoogleGlass/posts/aKymsANgWBD (Stand 10.01.2017).

7 Eine anschauliche Illustration zeigt die Media Disruption Map des Gottlieb-Duttweiler Instituts, http://www.gdi.ch/de/Think-Tank/Trend-News/Media-Disruption-Map-Innovationskraft-von-Medien (Stand 10.01.2017).

der Wahrnehmung der Nutzung von Datenbrillen im Vergleich zu etablierten Geräten (bspw. Smartphones) untersucht.

Dabei zeigte sich, dass die Nutzung von Geräten, die bereits länger kommerziell verfügbar sind, bei gleichem Verwendungszweck (z. B. zum Lesen von Kurznachrichten) einen höheren Akzeptanzwert erhielten, als die Datenbrille. Der vermutete Mangel an sozialer Akzeptanz konnte somit belegt werden.

Das Untersuchungsdesign[8] sieht zudem eine quantitativ messbare Metrik Szenario-bezogener sozialer Akzeptanz vor, was es ermöglicht, einen Wandel über einen längeren Zeitraum hinweg abzubilden. Durch eine wiederholte Messung über drei Jahre hinweg (4/2014, 4/2015, 4/2016) konnte gezeigt werden, dass bislang keine signifikante Zunahme positiver Einstellungen gegenüber Datenbrillen erfolgt ist.[9]

Als Ergebnis der Untersuchung der Einflussfaktoren ergab sich zudem, dass die Einschätzungen des Gerätenutzers und die der Umstehenden deutlich differieren.[10] Dies birgt gesellschaftliches Konfliktpotential: dieselbe Situation wird vom Datenbrillenträger selbst als weitaus weniger unangenehm und problematisch bewertet, als von dessen Gegenüber. Ein technisches System könnte an dieser Stelle ansetzen und durch das gezielte Unterbreiten von Vorschlägen und Hinweisen auf Seiten des Gerätenutzers ein Bewusstsein für dieses Problem schaffen (vgl. Kapitel 3.4).

Ein weiteres zentrales Ergebnis ist, dass sich das Sichtbarmachen der Nutzungsintention positiv auf die soziale Akzeptanz auswirkt. Heutige Geräte setzen dieses Prinzip (vgl. Kapitel 5.1) nicht oder nur teilweise um – zukünftige Entwicklungs- und Forschungsarbeiten haben daher hier anzusetzen und aufzuholen.

## 3 Design Achsen und Schlüsselfragen der Gestaltung

Smart Cams, die zwischen ihren Nutzern und deren Umfeld vermitteln und so einen Schutz der Privatsphäre der Umstehenden ermöglichen, ohne die Freiheit des Gerätenutzers zu beschneiden, werden vielfach gewünscht, sind jedoch ohne das vorherige Ausloten von Kompromissen nur schwer umsetzbar. Ein erster Versuch einer Festlegung von Design Achsen für diese Kompromissfindung (vgl. Abbildung 3) wurde von *Denning et al.*[11] auf der CHI 2014 vorgestellt.[12] Abbildung 2 zeigt den ursprünglichen Katalog an Design Achsen von *Denning et al.*, der auf Basis von in-situ Interviews mit Beobachtern und Beobachterinnen eines Datenbrillenträgers erstellt wurde. Aufbauend auf dem existierenden Katalog an Design Achsen wurden neun Schlüsselfragen abgeleitet, durch deren Beantwortung Lösungsansätze zur sozialakzeptablen Nutzung von Datenbrillen und Smart Cams generiert werden können. Nachfolgend werden verschiedene ausgewählte Technologieoptionen zur Beantwortung dieser Schlüsselfragen vorgestellt und diskutiert, sowie durch aktuelle Forschungsbeispiele ergänzt. Wo verfügbar, sind die zugeordneten, auf basierenden (englischsprachigen) Design Achsen in Klammern gesetzt.[13]

**Abbildung 2 | Design Achsen für die Kompromissfindung zwischen Privatsphärenschutz und Gerätenutzung[14]**

| | | |
|---|---|---|
| Push | | Pull |
| Proactive | | Reactive |
| Opt-in | | Opt-out |
| Recording-time | | Sharing-time |
| Compliance-dependent | | Compliance-independent |
| Enforced | | Suggested |
| Place-based | Proximity-based | Identity-based |
| User-based | Bystander-based | Third-party |
| Technical | Physical | Social |

### 3.1 Kommunikation

Ein wesentlicher Bestandteil der technischen Gestaltung des Verhaltens einer Smart Cam in einem Umfeld, in dem neben dem Gerätenutzer auch Unbeteiligte Dritte anwesend sind, ist die Art der Kommunikation zwischen den Teilnehmern.

► **Wie soll die Kommunikation zwischen Gerät, Gerätenutzer und Umstehenden gestaltet werden?**

Bei Verwendung einer Push Strategie (*push*) teilt das aufnehmende Gerät proaktiv mit, dass eine Aufnahme gemacht wird. Dies kann mittels einer digitalen Nachricht oder auch über ein Audio- oder Lichtsignal geschehen. Empfänger sind z. B. Personen oder Geräte innerhalb eines bestimmten Radius‘. Die Empfänger oder auch das empfangende Gerät können die Nachricht ignorieren, zur Kenntnis nehmen oder darauf reagieren (z. B. durch Senden einer Antwort). Im Gegensatz dazu wird bei einer Pull Strategie (*pull*) auf eintreffende Nachrichten gewartet bzw. je nach Implementierung in regelmäßigen Abständen bei Geräten im Umkreis angefragt. Eine Datenbrille könnte so beispielsweise die Präferenzen der Personen in einem bestimmten Umkreis (z. B.: „Benutzerin A möchte nicht auf Video aufgenommen werden.“) abfragen und entsprechend darauf reagieren (z. B. durch eine Benachrichtigung an den Nutzer oder durch automatisches Stoppen der Aufnahme). Die Mitteilung der Präferenzen durch die Umstehenden kann entweder automatisch (z. B. als Broadcast an alle

8 *Koelle/Kranz/Möller*, “Don’t Look at Me That Way!: Understanding User Attitudes Towards Data Glasses Usage”, in: *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*, New York 2015, S. 362–372.

9 *Koelle/Heuten/Boll/Kranz*, “All about Acceptability? Identifying Factors for the Adoption of Data Glasses”, in: *Proceedings of the ACM CHI Conference on Human Factors in Computing Systems*, Denver 2017.

10 *Koelle/Kranz/Möller*, “Don’t Look at Me That Way!: Understanding User Attitudes Towards Data Glasses Usage”, in: *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*, New York 2015, S. 362–372.

11 *Denning/Dehlawi/Kohno*, “In situ with Bystanders of Augmented Reality Glasses: Perspectives on Recording and Privacy-mediating Technologies”, in: *Proceedings of the 32rd Annual ACM Conference on Human Factors in Computing Systems*, New York 2014, S. 2377–2386.

12 Die ACM CHI Conference on Human Factors in Computing Systems ist mit einem CORE Ranking von A* die einflussreichste Konferenz im Bereich der Mensch-Maschine Interaktion.

13 *Denning/Dehlawi/Kohno*, “In situ with Bystanders of Augmented Reality Glasses: Perspectives on Recording and Privacy-mediating Technologies”, in: *Proceedings of the 32rd Annual ACM Conference on Human Factors in Computing Systems*, New York 2014, S. 2377–2386.

14 Nach *Denning/Dehlawi/Kohno*, “In situ with Bystanders of Augmented Reality Glasses: Perspectives on Recording and Privacy-mediating Technologies”, in: *Proceedings of the 32rd Annual ACM Conference on Human Factors in Computing Systems*, New York 2014, S. 2377–2386.

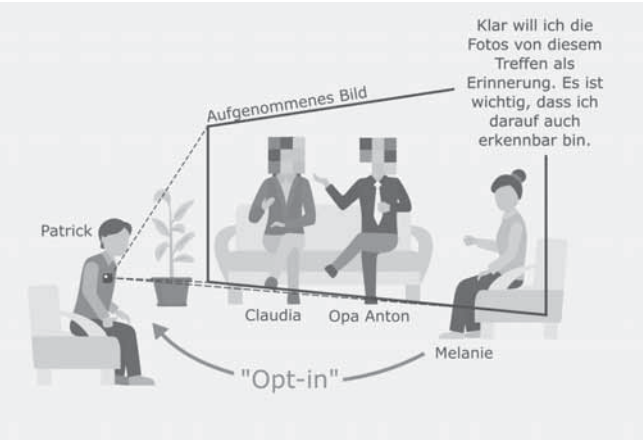
Geräte in der unmittelbaren Umgebung)[15] oder als Antwort auf eine Anfrage erfolgen.

► **Für wen ist der Status der Kamera sichtbar?**
Sichtbarmachen des Kamerastatus bedeutet, dass der Nutzer oder auch der/die Umstehende zu jedem Zeitpunkt sicher sagen kann, ob die Kamera gerade aufnimmt oder deaktiviert ist. Während dies für den Gerätenutzer insbesondere zu einer erhöhten Transparenz der Interaktion mit dem Gerät beiträgt, kann das Sichtbarmachen des Kamerastatus für die Umstehenden zum Abbau von Ängsten vor ungewollter oder unbemerkter Aufnahme beitragen und ihnen das Gefühl einer stärkeren Kontrolle zurückgeben. Eine weit verbreitete Methode der Anzeige sind visuelle Features am Gerät selbst (z. B. LEDs). Daneben ist auch der Einsatz einer Anzeigefunktion („Lookup") auf dem Gerät des Umstehenden selbst denkbar.[16] Ein (evtl. eingeschränktes) Sichtbarmachen des Systemstatus gegenüber Dritten (z. B. Behörden oder Betreibern von sozialen Netzwerken) ist technisch ebenfalls realisierbar. Diese Informationen können es z. B. erlauben, das Teilen von Aufnahmen zu unterbinden, die die Privatsphäre einer/eines Beteiligten beeinträchtigen würden.

► **Was ist aus der Anzeige des Status der Kamera ersichtlich?**
Neben dem reinen Sichtbarmachen des Kamerastatus stellt sich die Frage, was daraus (für die Umstehenden, aber auch für den Nutzer) ersichtlich sein soll bzw. darf. Eine binäre Anzeige des Kamerastatus erlaubt es abzuleiten, ob die Kamera gerade an („ON") oder aus („OFF") ist. Informationen darüber, was mit den aufgenommenen Daten passiert, sind nicht ersichtlich. Im Gegensatz dazu macht eine intentionsbasierte Anzeige sichtbar, wofür die Kamera gerade eingesetzt wird: wird das Kamerabild lediglich zum Zwecke des Trackings (z. B. von optischen Markern oder QR-Codes) kontinuierlich analysiert, aber nicht dauerhaft gespeichert? Dient die Aufnahme als Basis für Gesichtserkennung? Oder wird eine Aufnahme von Bild und Ton angefertigt?

Eine weitere denkbare Variante: die inhaltsbasierte Anzeige des Kamerastatus gibt Aufschluss darüber, was aufgenommen wird. Z. B. könnte zwischen Aufnahmen ohne Personen im Bild (z. B. Landschaft) und Aufnahmen mit einer oder mehreren Personen unterschieden werden. Basierend auf dieser Information könnten dem Gerätenutzer z. B. Vorschläge und Empfehlungen unterbreitet werden.

**Abbildung 3 | Illustration des Opt-in Prinzips. Als Beispiel einer Reaktion des Systems auf eine nicht vorhandene Einwilligung zur Aufnahme ist die Unkenntlichmachung des Gesichts durch „Verpixeln" dargestellt.**




## 3.2 Präferenzen

Bei der Gestaltung privatsphärensensitiver Technologien ist es relevant, wie die einzelnen Teilnehmer angeben, zu welchem Grad und vor wem sie ihre Privatsphäre schützen wollen: sie geben also – auf elektronischem Weg oder auch analog, z. B. mündlich – ihre ganz persönlichen Präferenzen an.

► **Wie teilen die Teilnehmer mit, ob bzw. von wem sie aufgenommen werden möchten?**
Eine sowohl grundlegende als auch problematische Frage im Kontext privatsphärensensitiver Smart Cams ist, ob die Aufnahme oder Nicht-Aufnahme (bzw. Unkenntlichmachung) einer Person als Standardwert (in der Informatik: Defaultwert) gilt. Bei einem Opt-in (*opt-in*) wird standardmäßig (per default) niemand aufgenommen. Eine Aufnahme findet nur bei expliziter Zustimmung statt. Dies kann z. B. bedeuten, dass alle Gesichter verpixelt dargestellt werden. Das Gegenteil von Opt-in ist Opt-out: standardmäßig (per default) wird jeder aufgenommen, der seine Zustimmung nicht explizit widerrufen hat. Eine Person, die nicht aufgenommen werden möchte, muss also über einen festgelegten Kommunikationsweg (z. B. über einen Onlinedienst, oder einen Marker) mitteilen, dass sie von der Kamera nicht aufgenommen werden möchte. Im Spielfilm „Operation Naked" von Mario Sixtus wird ein an der Stirn angebrachter QR-Code als optischer Marker eingesetzt,[17] aber auch für das menschliche Auge nicht wahrnehmbare Marker (NFC[18], oder Infrarot) sind dafür denkbar. In allen Fällen gilt: Teilnehmer, denen der für das Opt-in bzw. Opt-out vorgesehene Kommunikationsweg nicht zur Verfügung steht (z. B. weil sie kein Smartphone oder kein entsprechendes Token besitzen), können ihre Präferenzen nicht mitteilen und werden automatisch entsprechend der Standardeinstellung behandelt.

► **Wann teilen die Teilnehmer mit, ob bzw. von wem sie aufgenommen werden möchten?**
Werden Privatsphäre Präferenzen proaktiv (***proactive***) definiert, so bedeutet das, dass bereits bevor eine Aufnahme angefertigt wird bzw. werden kann, festgelegt wird, welche Maßnahmen zum Schutz der Privatsphäre der Teilnehmer ergriffen werden. Im gegenteiligen Fall, dem reaktiven (***reactive***) Festlegen von Präferenzen, erfolgt die Definition konkreter Privatsphäre-Einstellungen erst als Reaktion auf die Aufnahme bzw. die Begegnung mit dem Gerät. Eine solche Reaktion kann manuell oder auch automatisch erfolgen und z. B. beinhalten, dass der Ersteller eines Videos gebeten wird, dieses zu löschen oder den Zugriff zu beschränken.

15 *Barhm/Qwasmi/Qureshi/ El-Khatib*, „Negotiating privacy preferences in video surveillance systems", in: International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems, 2011; *Brassil*, „Technical challenges in location-aware video surveillance privacy", in: Protecting Privacy in Video Surveillance, London 2009.

16 Ein ähnliches Prinzip wurde bereits für CCTV Kameras umgesetzt: https://thecctvmap.wordpress.com/ (Stand 10.01.2017).

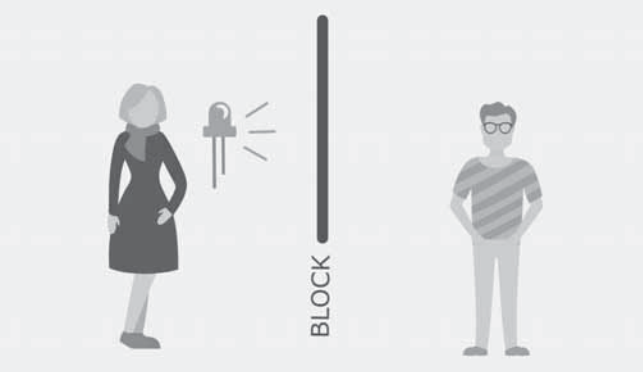
17 Operation Naked, ZDF, 2015, http://operationnaked.org/ (Stand 10.01.2017)

18 NFC, Abkürzung für „Near-Field Communication" bezeichnet einen Standard zum kurzzeitigen, kontaktlosen Austausch von Informationen zwischen zwei Geräten.

### 3.3 Umsetzung

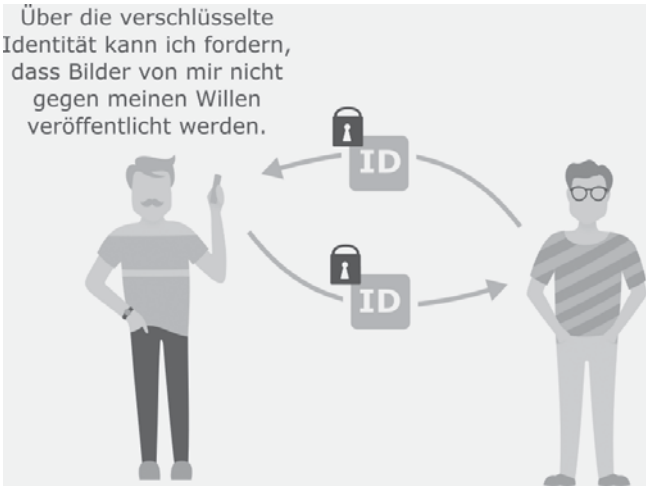
► **Wie wird der Schutz der Privatsphäre realisiert?**
Ein geräteabhängiger Schutz (*compliance-dependent*) der Privatsphäre basiert i. d. R. auf dem Austausch von Nachrichten. Dabei wird dem aufnehmenden Gerät (hier: Datenbrille) z. B. über Funk oder einen optischen Marker mitgeteilt, dass die Aufnahme des betreffenden Teilnehmers eingeschränkt werden soll, und das aufnehmende Gerät reagiert entsprechend. Diese Lösungen setzen die Kompatibilität und Kooperation des aufnehmenden Gerätes voraus. Eine Technologie, die die Aufnahme durch die Kamera eines Gerätes aktiv verhindert, ohne dass die Kooperation des Gerätenutzers oder des Gerätes selbst notwendig ist, nennt man geräte-unabhängig (*compliance-independent*). Infrarot Licht[19] oder Gesten können zu diesem Zweck eingesetzt werden, wie in Abbildung 4 illustriert. Ein auf diesem Prinzip basierendes System, welches sogenannte „BlindSpots" (vor Aufnahme geschützte Bereiche) schafft, wurde von *Patel et al.*[20] vorgestellt. Der Vorteil dieser Systeme liegt darin, dass keine Kompatibilität mit dem aufnehmenden Gerät vorausgesetzt werden muss.

**Abbildung 4 | Auch ohne Kooperation von Seiten des aufnehmenden Gerätes kann eine ungewollte Aufnahme verhindert werden – z.B. durch Infrarotlicht.**




► **An welche Parameter ist der Schutz der Privatsphäre gekoppelt?**
Technische Maßnahmen zum Schutz der Privatsphäre Umstehender können z. B. an die Parameter Ort (*place-based*), Abstand (*proximity-based*) und Identität (*identity-based*) gekoppelt werden. Eine ortsabhängige Beschränkung verhindert Kameraaufnahmen in einem bestimmten Raum, Gebäude oder Gebiet. Diese Einschränkung der Benutzung kann sowohl durch soziale Normen, das Aussprechen eines Verbotes (z. B. durch den Besitzer eines Lokals) oder auch durch technische Maßnahmen (bspw. Funksignale oder Geofences)[21] realisiert werden. Ein ortsbasiertes Verfahren ist immer an einen festgelegten physischen Bereich gebunden. Im Gegensatz dazu definieren abstandsbasierte Verfahren einen bestimmten Umkreis um eine bewegliche Entität (mobile Geräte, z. B. Datenbrillen). Innerhalb dieses Radius werden bestimmte Regeln angewendet, also zum Beispiel Maßnahmen zum Schutz der Privatsphäre von Individuen angewandt. Dies heißt auch, dass die Präferenzen bzgl. der Privatsphäre von Personen in der unmittelbaren Umgebung des Nutzers (z. B. im selben Raum) betrachtet werden, die von Personen im weiteren Umkreis (z. B. im selben Gebäude) aber nicht.[22]

**Abbildung 5 | Ein verschlüsselter, anonymer Austausch von IDs,[22] könnte verwendet werden, um unbemerkt oder ohne Zustimmung aufgenommene Bilder nachträglich löschen zu lassen, ohne die eigene Identität preiszugeben.**




Durch den (anonymen) Austausch von Identitäten (z. B. bei gleichzeitigem Aufenthalt an einem Ort)[23] könnte es dem Umstehenden ermöglicht werden, eine von ihm/ihr angefertigte und veröffentlichte Aufnahme zu jedem beliebigen Zeitpunkt nach deren Aufnahme bzw. Veröffentlichung aus dem Netz nehmen zu lassen, eine Markierung („Tag") zu entfernen oder den Zugriff zu beschränken.[24] Ebenso ist der Abgleich von Präferenzen auf Basis der (anonymen) Identität möglich, wie in Abbildung 5 illustriert.

### 3.4 Durchsetzung

► **Wie werden die Präferenzen der Teilnehmer bzgl. deren Privatsphäre durchgesetzt?**
Die Wahrung der Privatsphäre kann durch technische Maßnahmen (*technical*) sichergestellt werden.[25] Unerwünschte Bild- oder Videoaufnahmen können zudem dadurch verhindert werden, dass die Aufnahme physisch unmöglich gemacht wird (physical). Möglichkeiten sind das Verbot der Mitnahme bzw. des Tra-

19 Das Projekt Camoflash des Künstlers Adam Harvey setzt Infrarot LEDs ein, um ungewollte Fotografien zu verhindern: https://ahprojects.com/projects/camoflash/ (Stand 10.01.2017)

20 *Patel/Summet/Truong*, „Blindspot: Creating capture-resistant spaces", in: Protecting Privacy in Video Surveillance, London 2009.

21 Ein Geofence (Kunstwort aus *geographic* [engl. geographisch] und *fence* [engl. Zaun]) bezeichnet einen klar umrissenen, geographischen Bereich, auf dessen Basis ein Geoinformationssystem bestimmen kann, ob sich eine Entität (z.B. eine Smart Cam) innerhalb oder außerhalb der festgelegten „Umzäunung" befindet.

22 Vorgeschlagen von *Manweiler/Scudellari/Cancio/Cox*, „We saw each other on the subway: secure, anonymous proximity-based missed connections", in: 10th workshop on Mobile Computing Systems and Applications, 2009.

23 *Manweiler/Scudellari/Cancio/Cox*, „We saw each other on the subway: secure, anonymous proximity-based missed connections", in: 10th workshop on Mobile Computing Systems and Applications, 2009.

24 Vgl. *Besmer/Lipford*, „Moving Beyond Untagging: Photo Privacy in a Tagged World", in: *Proceedings of the ACM CHI on Human Factors in Computing Systems*, New York 2010, S. 1563-1572

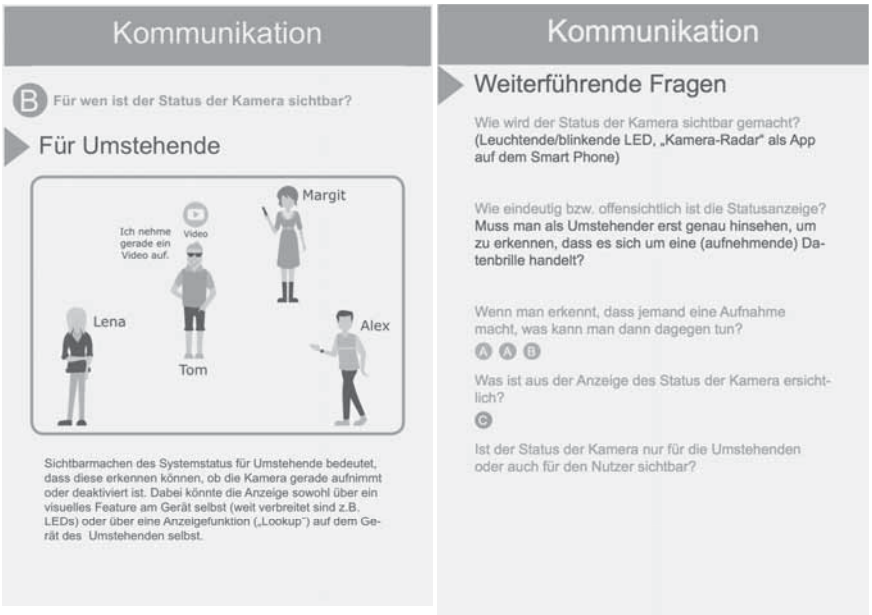
25 Ein ausführlicher Überblick über Methoden der technischen Unkenntlichmachung von abgebildeten Personen ist nachzulesen bei *Padilla-López/Chaaraoui/Flórez-Revuelta*, „Visual Privacy Protection Methods: A Survey," Expert Systems with Applications, Bd. 42, Nr. 9, 2015, S. 4177-4195.

gens des Gerätes oder das physische Abdecken oder Abkleben der Linse. Selbstgemachte, z. T. auch humoristische Lösungen (z. B. das Glass Privacy Cover)[26] zeigen, dass es ein Bedürfnis nach einem intuitiv erkennbaren Schutz vor Aufnahme gibt. Wird die Aufnahme weder technisch noch physisch verhindert, so kann dennoch durch soziale (*social*) oder gesetzliche Normen[27] ein Schutz der Privatsphäre Einzelner erreicht werden. Es ist in diesem Fall jedoch immer eine persönliche Entscheidung des/der Einzelnen, ob er/sie sich an die soziale Norm hält oder sich darüber hinwegsetzt und mögliche Konsequenzen in Kauf nimmt.

- **Wie bindend sind die Präferenzen anderer Teilnehmer bzgl. deren Privatsphäre für den Gerätenutzer?**

Maßnahmen zum Schutze der Privatsphäre anderer können dem Nutzer eines Gerätes als Vorschlag (***suggested***) unterbreitet werden. Wird eine mögliche Missachtung der Privatsphäre eines Dritten erkannt, so kann das System den Nutzer automatisiert darauf hinweisen und eine mögliche, sozialakzeptierte Reaktion (z. B. das Ausschalten des Geräts oder das Nichtveröffentlichen der Aufnahme) vorschlagen. Wird der Schutz der Privatsphäre im Gegensatz dazu als verpflichtend definiert, so kann erzwungen (***enforced***) werden, dass der Nutzer eines Gerätes entsprechende Schutzmaßnahmen durchführt oder sich an bestimmte Bestimmungen hält und z. B. eine Aufnahme nicht veröffentlicht. Dies kann technisch von Seiten des Systems (z. B. durch Unterbinden der Aufnahme oder durch hardwareseitiges unkenntlich Machen von Gesichtern) oder auch durch den Gesetzgeber (z. B. durch Androhung von Strafen) durchgesetzt werden.

**Abbildung 6 | Vorder- und Rückseite einer „Privacy Mediation Card": Sichtbarkeit des Kamerastatus für Umstehende**




## 4 Partizipative Erhebung von Lösungsvorschlägen

Nachdem die zentralen Einflussfaktoren für die soziale Akzeptanz untersucht wurden, geht es um die Frage einer technischen Lösung. Durch die Entwicklung neuer interaktiver Konzepte von Form und Funktion der Kameras soll die Verringerung der Ablehnung und Erhöhung der sozialen Akzeptanz beeinflusst werden. Ansatz ist eine Entwicklung von Form und Funktion, die es den Umstehenden besser ermöglicht einzuschätzen, ob, wann und was aufgezeichnet wird und wie ggf. auch auf die Aufnahme Einfluss genommen werden kann. Ein methodischer Ansatz ist hierzu das sogenannte Partizipative Design, das die zukünftigen Nutzerinnen und Nutzer aktiv in den Gestaltungsprozess mit einbezieht.[28]

### 4.1 Aufbereitung des Stands der Technik

Vorhergehende Studien[29] haben gezeigt, dass insbesondere bezüglich der tatsächlichen technischen Fähigkeiten von Datenbrillen und Smart Cams bei vielen, technisch weniger versierten – „Laien" – große Unsicherheiten und sogar Fehlannahmen bestehen. Zudem ist die Bandbreite der technologischen Möglichkeiten umfangreich und erstreckt sich über mehrere Forschungsfelder, u. a. Datensicherheit und Verschlüsselung, Bildverarbeitung und Computer Vision sowie Industriedesign.

Um eine Diskussionsgrundlage für Nicht-Technologieexperten zu schaffen, wurde aufbauend auf den hergeleiteten Schlüsselfragen (vgl. Kapitel 3) ein Kartenset entwickelt, das Technologieoptionen für die sozialakzeptable Nutzung von Smart Cams veranschaulicht sowie weiterführende Fragen aufzeigt. Ein Beispiel einer Karte aus dem „Privacy Mediation" Kartenset ist in Abbildung 6 dargestellt. Diskussionsteilnehmer können so anhand vorgegebener Möglichkeiten Szenarien entwerfen, die sie für sozial akzeptabel halten, und anhand der gegebenen weiterführenden Fragen diskutieren und auf Konsistenz überprüfen.

### 4.2 Einsatz der Fokusgruppendiskussion als partizipative Designmethode

Die Teilnehmer waren Studierende unterschiedlicher fachlicher Ausrichtungen.[30] Im Anschluss an einen 60-minütigen Impulsvortrag wurden die Teilnehmenden in fünf 3er Gruppen aufgeteilt, um zu diskutieren, wie existierende (oder auch konzeptio-

26 John Biehler, „Google Glass Privacy Cover" auf Thingiverse: http://www.thingiverse.com/thing:182763 (Stand 10.01.2017).

27 Hierzu die Beiträge Rose und Bischof in diesem Heft.

28 In Rahmen eine interdisziplinären, studentischen Konferenz fand eine Einführung statt, um erste, partizipativ generierte Vorschläge zu sammeln, wie eine sozialakzeptable Nutzung von Smart Cams und Datenbrillen technisch umgesetzt werden kann und aus Nutzersicht umgesetzt werden soll. Im Sinne des sogenannten partizipativen Designs wurden die Workshop Teilnehmer angeleitet, in Kleingruppen potentielle Lösungswege zu entwickeln, zu diskutieren und zu bewerten.

29 *Koelle/Kranz/Möller*, "Don't Look at Me That Way!: Understanding User Attitudes Towards Data Glasses Usage", in: *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*, New York 2015, S. 362–372.

30 Fünfzehn Teilnehmer im Alter von 18 bis 28 Jahren ($\bar{x} = 23$, $\sigma = 3{,}44$), 4 davon männlich, nahmen an einer 120-minütigen Fokusgruppendiskussion teil.

nelle) Technologien und Regelungen eingesetzt werden können, um eine sozial akzeptierte Nutzung von Augmented Reality und anderen kamerabasierten Anwendungen zu ermöglichen. Mit Hilfe des zu diesem Zwecke entwickelten Kartensets (den sogenannten Privacy Mediation Cards, siehe Kapitel 2) gestalteten die Teilnehmer ihren eigenen Wünschen und Vorstellungen entsprechende Lösungsszenarien. Im Anschluss wurden die Ergebnisse der Diskussion im Plenum präsentiert.

### 4.3 Ergebnisse der Fokusgruppendiskussion

Die Diskussionen während des Workshops haben gezeigt, dass die sozialakzeptable Nutzung von Smart Cams ein kontroverses Thema mit hohem Konfliktpotential ist, zu dessen Lösung es weiterer wissenschaftlicher und gesellschaftlicher Bemühungen bedarf. Kontrovers diskutiert wurde u. a. der Konflikt zwischen dem Wunsch nach einer unverfälschten Aufnahme im Rahmen künstlerischer Freiheit und dem individuellen Schutz vor ungewollter Aufnahme durch Andere. Nachfolgend gewähren wir erste Einblicke in Diskussionsinhalte und zeigen daraus abgeleitete Erkenntnisse auf.

#### Gleichgewicht zwischen Einschränkungen des Nutzers und der Privatsphäre Dritter

Die Teilnehmer der Diskussionsgruppen machten deutlich, dass sie zwar die Privatsphäre Dritter mit Hilfe technischer Maßnahmen schützen wollen, gleichzeitig aber die Einschränkung des Nutzenden des jeweiligen Gerätes auf ein Minimum reduzieren möchten (G2, G4, G5). Während eine der Kleingruppen sich für ein komplettes Verbot der Nutzung in der Öffentlichkeit aussprach, beurteilte eine der anderen Gruppen die Veröffentlichung des Bildmaterials als den kritischsten Aspekt und gab an, dass das Erstellen und Aufbewahren dieser Materialien nicht verboten sein sollte. Dieser Konflikt wurde auch deutlich bei der Kommunikation von Privatsphärepräferenzen, also wie die einzelnen Teilnehmer mitteilen, ob bzw. von wem sie aufgenommen werden möchten. Eine der fünf Gruppen befürwortete ein reines Opt-in, um die Privatsphäre aller Umstehenden zu schützen. Zwei Gruppen verfolgten hingegen einen konträren Ansatz: Sie waren für ein Opt-out. Sie begründeten dies mit der Praktikabilität der Gerätenutzung und argumentierten, dass es viele passive Teilnehmer gäbe, die nicht aktiv ihr Einverständnis gäben, da es ihnen gleichgültig sei, ob sie gefilmt würden oder nicht.

#### Entscheidend sind Ort und Intention der Nutzung

Alle Gruppen waren sich einig, dass es Orte geben sollte, an denen die Aufnahme von Bildmaterial generell verboten ist. Allerdings verfolgten die einzelnen Gruppen verschiedene Ansätze der Umsetzung. Vorschläge reichten vom rigorosen Verbot aller kamerabasierten Anwendungen in der Öffentlichkeit, bis hin zum selbstständigen Abwägen und Entscheiden des Nutzers. Auch die Nutzungsintention wurde als ausschlaggebend bewertet. Demzufolge würden Aufnahmen in Krankenhäusern zwar generell verboten, Ausnahmeregelungen für bspw. Familienfotos jedoch ermöglicht.

#### Visualisierung des Kamerastatus

Die Teilnehmenden diskutierten, ob der Kamerastatus Außenstehenden angezeigt werden soll oder nicht. Von vier der fünf Gruppen wurde der Vorschlag gemacht, den Kamerastatus mithilfe von verschiedenfarbigen LEDs zu kommunizieren. Eine Gruppe ging sogar so weit, auf der Datenbrille anzuzeigen, wie die nutzende Person sie gerade einsetzt. Dieser Vorschlag stieß aber auf Widerstand, da dies ein zu großer Eingriff in die Privatsphäre des Nutzers sei.

#### Verantwortung für den Schutz der Privatsphäre

Als ein mehrfach hinterfragtes und kontrovers diskutiertes Problem stellte sich die Durchsetzung des Privatsphärenschutzes durch Hersteller, gesellschaftliche Normen und gesetzliche Regelungen heraus. Speziell die Überprüfung verschiedener Einzelfälle durch den Gesetzgeber wurde von den Teilnehmern als problematisch erachtet. Ein Teilnehmer (Gr. 2) sagte hierzu: „*Vor allem gäbe es dann so unglaublich viele Fälle, die eigentlich nicht von Bedeutung sind, aber dadurch rechtswidrig, dass wahrscheinlich Fälle, [die] von Bedeutung, aber rechtswidrig [sind], nicht verfolgt werden. Also da wirklich eine rechtliche Grundlage, die auch durchsetzbar ist, zu erstellen, scheint mir recht schwierig.*“

## 5 Fazit

Mit unseren bisherigen Forschungsarbeiten konnten wir zeigen, dass Datenbrillen und Smart Cams trotz des großen öffentlichen Interesses und der fortschrittlichen Technologie noch nicht gesellschaftlich akzeptiert sind bzw. werden können. Als Kernfragen haben sich dabei die Sichtbarmachung der Interaktion und Darstellung des Kamerastatus sowie das Finden von geeigneten Mechanismen zur Festlegung und Kommunikation von Privatsphärenpräferenzen herausgestellt. Um eine sozialakzeptable Nutzung dieses Gerätetypus zu ermöglichen, ist die Entwicklung von Lösungsansätzen, die sich mit den in diesem Artikel vorgestellten Schlüsselfragen auseinandersetzten, zwingende Voraussetzung. Wichtig ist dabei, dass die Lösungsfindung schlussendlich nicht nur mit Sicht auf die technische Realisierbarkeit, sondern auch unter Einbezug der Nutzerbedarfe angegangen wird: die sozialakzeptable Nutzung von Smart Cams und Datenbrillen ist nicht nur eine technologische, sondern auch eine gesellschaftliche Herausforderung.