Privacy and Security Issues and Solutions for *Mixed Reality* Applications

7

Jaybie A. De Guzman, Kanchana Thilakarathna, and Aruna Seneviratne

Contents

Abstract

Mixed-reality (MR) technology development is now gaining momentum due to advances in computer vision, sensor fusion, and realistic display technologies. Despite this, most of the research and development has been focused on delivering the promise of MR; concerns on potential *security* and *privacy* risks are continuously being pointed out, and only a few are working on the privacy and security implications of the technology. We put into light these risks and look into the latest security and privacy work on MR. In this chapter, we present an exposition and categorization of the latest security and privacy work on MR.

Keywords

Augmented reality · Mixed reality · Virtual reality · Security · Privacy · Usability in security and privacy · Safety · Survey · Spatial data · 3D data · Computer vision · Collaborative interactions

J. A. De Guzman (✉)
University of the Philippines Diliman, College of Engineering Electrical and Electronics Engineering Institute, Quezon City, Philippines
e-mail: jaybie.de.guzman@eee.upd.edu.ph

K. Thilakarathna
The University of Sydney, School of Computer Science Faculty of Engineering, Sydney, NSW, Australia
e-mail: kanchana.thilakarathna@sydney.edu.au

A. Seneviratne
University of New South Wales, School of Electrical Engineering and Telecommunications, Sydney, NSW, Australia
e-mail: a.seneviratne@unsw.edu.au

7.1 The Mixed Reality Present

The future with *mixed reality* (MR) is now. Starting 2015 or even earlier, we have seen an increase in *augmented* (AR) and *mixed reality* (MR) devices and applications either using head-worn or hand-held form factors. With Apple's release of the ARKit SDK for the iOS during the 2018 Apple Worldwide Developers Conference, and, soon after, Google followed with ARCore for Android, the year 2019 saw a boom in hardware and software platforms that aim to bring MR to the mainstream. In this chapter, we will refer to augmented, virtual, and mixed reality, collectively, as mixed reality or MR.

The Current Focus with MR Majority of the research and development efforts over MR have primarily been on delivering the technology: specifically on improving the visual experience and the mobility of these services. Early surveys on MR have focused on categorizing or determining these necessary technologies. In 1994, a taxonomy for classifying MR displays and platforms based on the user interface and plotting these devices along a reality-virtuality continuum was presented [1]. Subsequent classifications were also presented based on the concepts of transportation (the extent to which the users are transported from their physical locality to a virtual or remote space), artificiality (the extent to which the

A. Y. C. Nee, S. K. Ong (eds.), *Springer Handbook of Augmented Reality*, Springer Handbooks,
https://doi.org/10.1007/978-3-030-67822-7_7

user space has been synthesized from a real physical space), and spatiality (the extent to which properties of natural space and movement are supported by the shared space) [2]. Consequently, a survey has identified and discussed the various early challenges in MR: specifically focusing on physical-virtual alignment, optical distortion, and object tracking [3]. It was complemented with a follow-up survey that focuses on the enabling technologies, interfacing, and visualization [4]. Another recent survey updated the challenges in MR systems to include performance, interactions, and mobility [5]. Again, While it is important to highlight these classifications and challenges, it is also equally important to highlight the security and privacy issues and solutions in MR.

Nonetheless, a few recent works have pointed out the ethical considerations [6] as well as value-sensitive design approaches that consider data ownership, privacy, secrecy, and integrity [7]. Another recent study has highlighted the potential perceptual and sensory threats that can arise from MR outputs, such as photosensitive epilepsy and motion-induced blindness [8]. Moreover, a relevant recent work has emphasized the *input*, *data access*, and *output* aspects for protection in MR [9]. In a recent survey on MR security and privacy approaches, we have extended these to include *interaction* and *device* protection as equally important aspects [10]. Now, in this chapter, we will present a re-categorization of these aspects and update the collection with the latest security and privacy work over MR.

7.1.1 Overview on Mixed Reality Processing

Figure 7.1 shows a generic pipeline for MR processing. MR platforms collect information through sensors that may capture various signals from the environment. MR has particularly put emphasis on visual information as the primary mode of information and experience. The captured visual or spatial information are processed to construct machine-understandable representations of these information. Common examples include a spatial mapping (or digital representation) of the environment, or a skeletal abstraction of user anatomy for gesture detection. This allows the MR platform to have an environmental understanding and detect the information-of-interest, which can be a structural feature

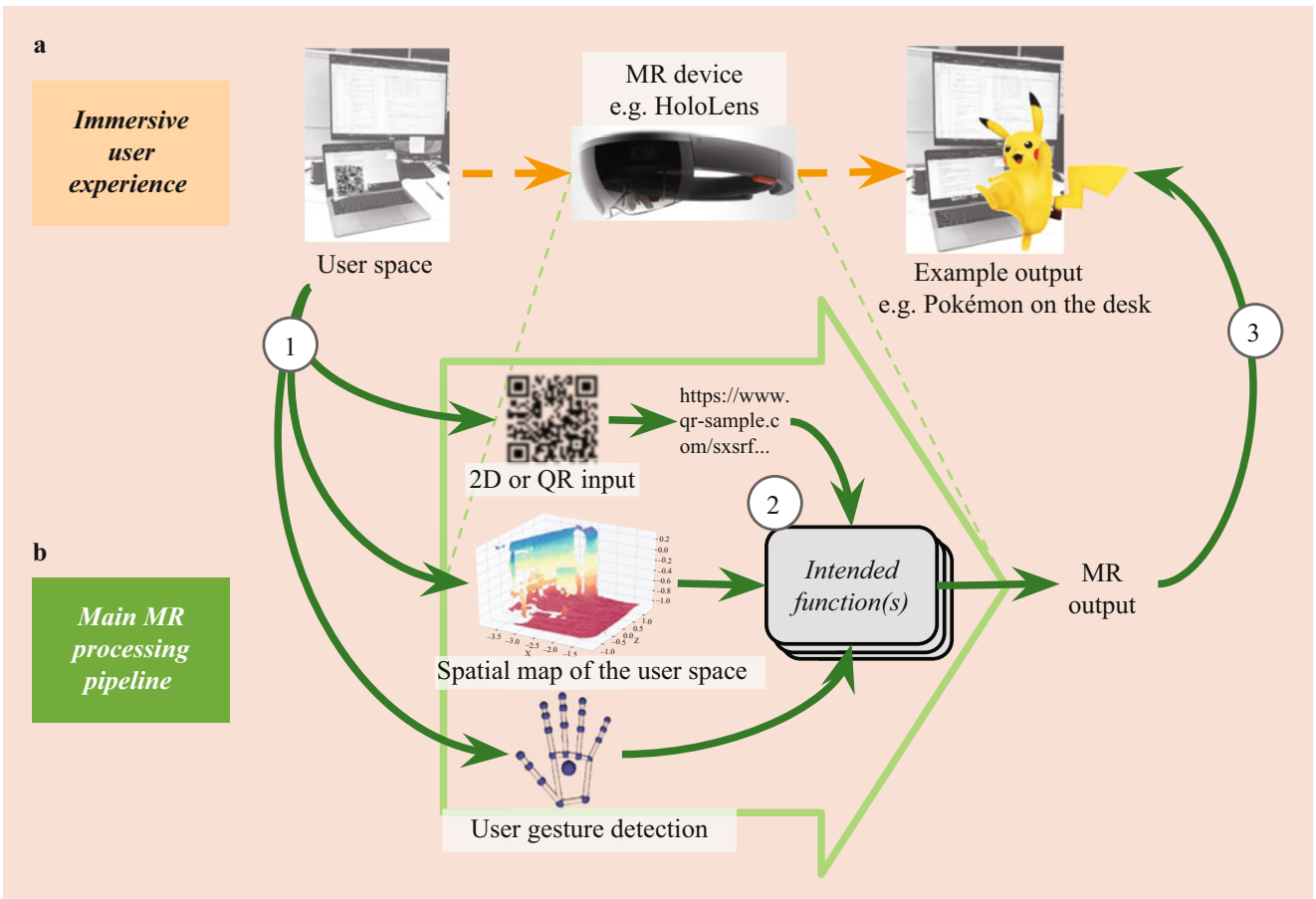

Fig. 7.1 Mixed Reality pipeline: (**a**) the immersive experience as viewed by the user; (**b**) the main processing pipeline of (1) detection or sensing, (2) transformation, and (3) rendering or actuation

(e.g., wall and floor), visual target (e.g. 2D QR code, or an actual object), or user gesture (e.g., hand or eye movement). Then, the MR application extracts the necessary information (e.g., object orientation in space), which are transformed to usable information (e.g., virtual features that can be anchored by virtual objects). Finally, the MR output is rendered on to the scene to make it seem like it inhabits the real world as it is viewed through a display. Spatial audio may also be added for an immersive MR experience.

7.1.2 Towards MR Mobility

Given that our mobile hand-held devices are primarily used for non-MR applications, it is only apt that new and dynamic ways of processing need to be designed to handle the processing demands of MR. More so that MR is one of these upcoming services that expected to further push the limits of hand-held devices and cloud computing. For example, Microsoft now offers remote rendering for the HoloLens through their Azure cloud service for rendering more complex 3D models, especially those used in engineering and architecture.

Various recent works on cloud- and edge-assisted MR processing include the reverse offloading processing back to the user devices as edge computing devices to alleviate cloud infrastructure cost and reduce latency [11,12], utilizing GPU acceleration with cloud offloading [13], or using convolutional neural networks (or CNN) for object detection in the cloud [14]. While most of these works were mostly on 2D (i.e., image-based) data, it is also necessary to investigate actual 3D detection, such as those specifically used by current MR platforms as listed in Table 7.1, particularly looking at how auxiliary servers can be utilized for offloading 3D processing tasks. Perhaps, we can look towards techniques proposed in the area of vehicular AR for improving vehicular visibility collaboratively [15]. Likewise, we may also look towards efforts in wireless virtual reality (VR) for remote 3D rendering [16].

Ultimately, all these developments in mobile MR processing needs to be scrutinized in terms of the privacy and security risks that these developments may pose to the users. As we proceed in this chapter, we will present an overview of the various security and privacy risks that MR poses. Afterwards, we will present a review of the various approaches as well as a categorization of these approaches. Then, we present the remaining challenges that need to be addressed before finally concluding the chapter.

7.2 Security and Privacy Risks with Mixed Reality

Given these capabilities and the continuous development in machine vision and sensor fusion technologies, MR users face even greater risks as richer information can be gathered using a wide variety of methods. For example, the Microsoft HoloLens has a multitude of visual sensors: four (4) cameras for environment understanding, a separate depth sensor, two (2) infrared cameras for eye tracking, and another camera for view capture. Figure 7.2b shows an example of spatial map captured using HoloLens. These spatial maps are more memory-light than video despite containing near-accurate 3D digital representations of user spaces. Once these information are made available to applications and services, users may no longer have control over how these data are further utilized.

7.2.1 Risks with MR Data Processing

Despite these capabilities being seemingly necessary in delivering the promise of MR, not all MR functionalities or services require extremely rich information. Privacy concerns are further exacerbated by recent advances, such as near-real-time visual object detection using machine learning, which enables inference beyond the intended functionality [17]. For example, visual sensors in the MR device can subtly capture images and video without the knowledge of those around the user. This violates bystander privacy or the unauthorized capture of information about the other users, or so-called bystanders. Moreover, it has been demonstrated how easy it is to use a simple facial recognition algorithm to match live-captured photos with publicly available photos online (from online social networks such as Facebook) and extract personal information such as names and social security numbers [18]. Various endeavors have highlighted these risks over captured visual data, and likewise, various protection mechanisms have been posed.

Risks with 3D Spatial Data However, it is not only visual data that poses risks but also the spatial maps that provide the necessary environment understanding to MR platforms. This

Table 7.1 API class or command handling 2D and 3D detection

Software platform	2D	3D	Shareable?
Google's ARCore	*AugmentedImage*	*Trackables*	Yes, via *CloudAnchors*
Apple's ARKit	*ARReferenceImage*	*ARWorldTracking*	Yes, via *ARAnchors*
Window's MR API 2	No native support from API but can use any third party library or API that can run on Windows	*SpatialMapping*	Yes, via *SpatialAnchors*

Fig. 7.2 Comparison of different representations of the (**a**) physical environment: (**b**) the captured spatial map, which is stored as an unordered list of 3D points and usually accompanied by triangle mesh information to represent surfaces; (**c**) the rendered digital map with a color texture extracted from image captures to create an almost accurate copy of the physical space. (**a**) Real representation. (**b**) 3D digital representation. (**c**) Rendered reconstructed representation

capability further poses unforeseen privacy risks to users. Once these captured 3D maps have been revealed to untrusted parties, potentially sensitive spatial information about the user's spaces is disclosed. Adversaries can vary from a benign background service that delivers unsolicited advertisements based on the objects detected from the user's surroundings to malevolent burglars who are able to map the user's house and, perhaps, the locations and geometry of specific objects in their house based on the released 3D data. Furthermore, turning off GPS tracking for location privacy may no longer be sufficient once the user starts using MR applications that can expose their locations through the 3D and visual data that are exposed. For example, Google has unveiled a *Visual Positioning Service* (or VPS) using visual and 3D data to locate users—an offshoot of Project Tango—during their 2018 I/O keynote event.

User Perception of 3D Spatial Data With images and video, what the "machine sees" is practically what the "user sees," and a great deal of privacy work have been done on these data forms. Contrariwise, in most MR platforms, the experience is exported as visual data (e.g., objects augmented on the user's view), while the 3D nature of the captured spatial data is not exposed to the user: what the machine sees is different—arguably, even more—from what the user sees. That is, the digital representation of the physical world that the machine sees and understands is not exposed to the user. This inherent perceptual difference creates a latency from user perception and, perhaps, affects the lack of user-perceived sensitivity over the captured spatial information.

Moreover, no privacy preservation is currently applied before providing these spatial data to third-party applications. Aside from the spatial structural information, the mapping can also include 3D maps of objects within the space. Figure 7.2b shows that the digital representation not only accurately models the real representation but also includes information regarding the orientation of objects in the user environment at the time of interaction. Even the slightest change in the orientation will result in a different 3D point data, allowing the MR machine to detect such changes that otherwise would have been unnoticeable to a human eye—hence 'seeing' more than human perception.

Since users cannot readily understand how the machine sees in 3D, we speculate that users might inherently not bother with the sensitive information that 3D MR data captures. A recent study explored users' concerns in a multi-user MR environment where they highlighted the lack of concern from participants about how the technology can be maliciously used by other users and applications [19]. However, further study on the differences of user perception between 2D and 3D data representations as well as comparison of privacy concerns between the two need to be conducted to further corroborate our previous speculation.

Furthermore, despite the varying underlying vision processing algorithms employed, most of these MR platforms directly operate on these 3D spatial maps and offer cross-platform interoperability. Table 7.1 lists three APIs or SDKs for three popular MR platforms. It shows how each MR software platform handles, or which command or class handles, 2D and 3D detection. Due to the inherent differences in the algorithms used for 2D and 3D detections, separate commands or classes are used; however, they have cross-platform interoperability for visual anchors as presented in the last column. These visual anchors can be shared online between users of different MR platforms. However, the interoperability may pose new security and privacy risks.

7.2.2 Mobility and Privacy

In Sect. 7.1.2, various strategies in mobile MR processing were discussed to primarily distribute MR processing to reduce latency and provide a better mobile MR experience.

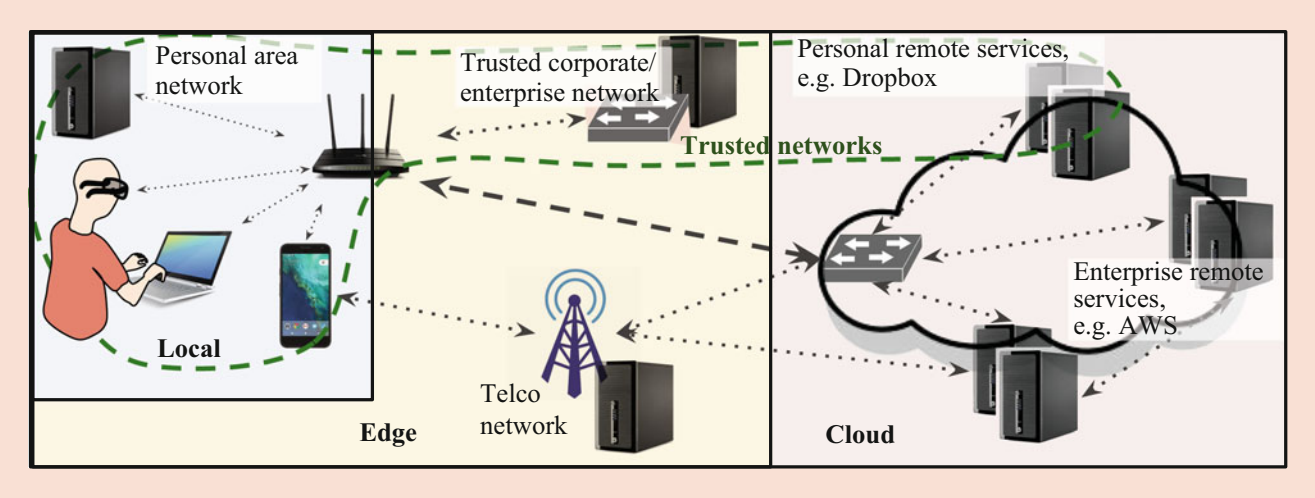

Fig. 7.3 Network of local devices, edge, and cloud auxiliary servers. A trusted subnet of this network is also shown, which is encircled by the green broken line

However, offloading the user data to remote edge and cloud servers may introduce risks. Enterprise networks or cloud storage servers may be considerably safe, but the trustworthiness of edge devices cannot be ensured. In general, as seen in Fig. 7.3, as we move away from the user device, the processing capacity increases, but the trustworthiness may not necessarily be ensured.

In order to investigate how much data were being offloaded by current MR apps, we performed packet transaction type analysis over a number of ARCore, ARKit, and Hololens applications. We used the following transaction-type categories: Application (`App`), Utilities (`Utilities`), and Advertising and Analytics (`Ads&Analytics`). We also separated transactions into download (`DL`) or upload (`UP`) to obtain the ratio of data packets being offloaded. Figure 7.4 shows that, while packets related to advertising and analytics were seen in each of the investigated ARCore apps, packets under this category are mostly not present in the current MR apps. Not only are the observed packet transaction lengths predominantly related to MR processing-and-services but also seem to be mainly used for offloading packets to auxiliary servers in some applications, such as HoloLens' holotour. These findings therefore highlight the potential privacy and security threats users are exposed to while using MR apps and affirm the need for countermeasures to ensure user privacy and security.

7.3 Protection Approaches for Mixed Reality

As vision processing and mobility are both being addressed and discussed well, privacy remains as a big challenge for MR. Given the sensing power and capabilities of MR, nascent as well as unknown privacy and safety risks arise. Now, we will present the various security and privacy works in MR according to the subsequent categorization discussed below.

Categorizing the Approaches Figure 7.6 shows an example MR environment with sample target elements for protection. Physical entities (e.g., desk, cup, or keyboard) from the environment are captured or detected. After detection, the resulting entities will be transformed or processed to deliver services accordingly. Depending on the service or application, different transformations are used. Finally, the results of the transformation are delivered to the user by rendering them (such as the virtual pet bird or the cup-contents indicator) through the device's output interfaces.

Figure 7.5 shows the four categories (and their subcategories) to which we will distribute the various related works. The first two categories of *input* and *output* protection are directly mapped to the associated risks with the *detection* and *rendering* stages of the MR processing pipeline, respectively. While *interaction* and *device* protection cannot be directly mapped along the pipeline but can be visualized within an MR environment as labeled in Fig. 7.6.

Table 7.2 lists the security and privacy properties, associated threats, and definitions. We follow the same combined list of properties that were presented in our original survey paper [10]. The top six properties are security-oriented, while the lower six are considered as privacy-oriented. The confidentiality property is considered both a security and privacy property. Consequently, some security properties are conversely considered as privacy threats and vice versa: for example, non-repudiation is the "threat" to plausible deniability. Nonetheless, these properties are not necessarily

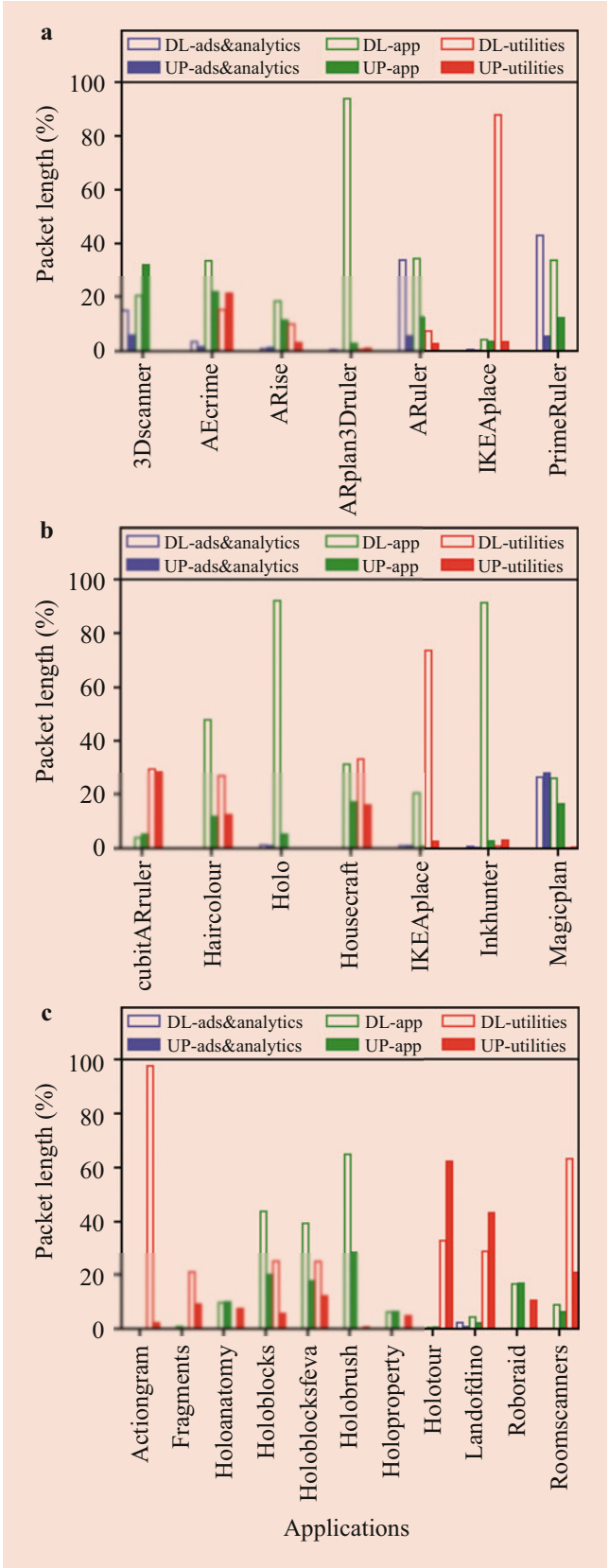

Fig. 7.4 Upload(UP) and download(DL) packet length distribution of MR apps to generalized categories in the first 5 min of app usage. NOte: This experiment was conducted in May 2019 (**a**) ARCore. (**b**) ARKit. (**c**) Hololens

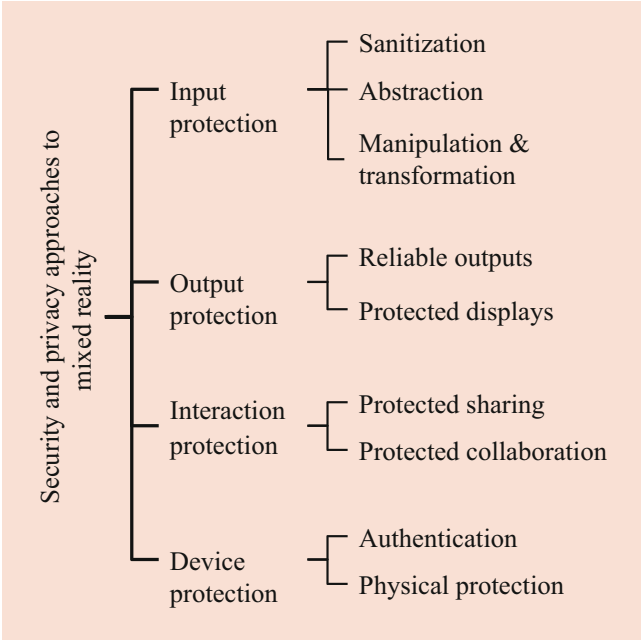

Fig. 7.5 A data-centric categorization of the various security and privacy work or approaches on mixed reality and related technologies

mutually exclusive and may be desired at the same time and, thus, be applied to different elements along the processing pipeline.

7.3.1 Input Protection

Several MR and related PETs have been proposed in the literature, and most of these early privacy works focused on 2D visual data protection (Fig. 7.7).

Visual Information Sanitization

Early approaches primarily involved applying sanitization techniques on visual media (i.e., image and video), e.g., selective blurring, replacement, or outright removal of sensitive portions in images or video frames. Sanitization removes latent and sensitive information from the input data stream. Various approaches use different methods to sanitize sensitive visual information, e.g., removing RGB and only showing contours [20]; detecting markers that signify sensitive content to be sanitized [21, 22], based on context [23, 24] or through user gestures [25]; or mechanically blocking the visual feed [26]. However, these methods only employ intrinsic policy enforcement or are "self-policing," which can potentially have a myopic view of privacy preferences of external objects. Thus, other works have focused on extrinsic policy enforcement to allow objects (including other users who are so-called bystanders) to communicate their privacy preferences. An early implementation [27] involved outright capture interference to prevent sensitive objects from being

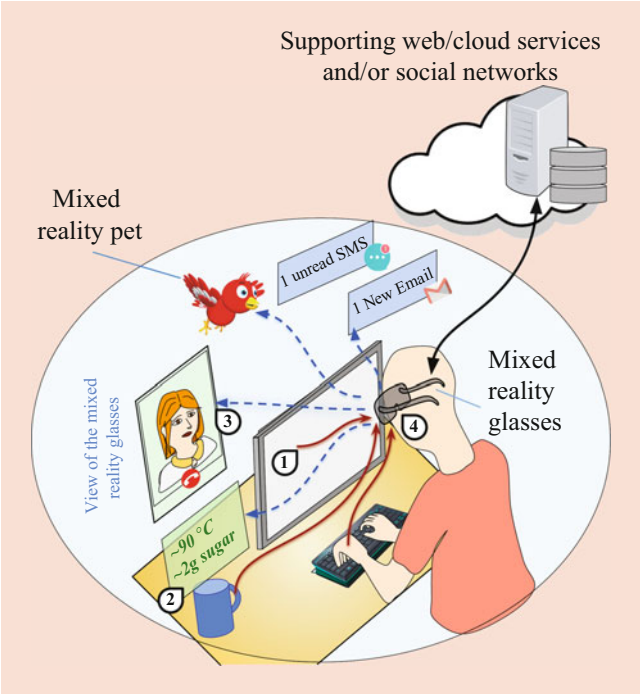

Fig. 7.6 A *mixed reality environment* with example points of protection as labeled: (1) *inputs* such as contents of the display monitor, (2) *rendered outputs* such as virtual display of a smart mug, (3) interactions such as collaborating with other users, and (4) *device* access to the mixed reality eyewear

captured by unauthorized visual capturing devices. It uses a camera that detects other cameras and flashes a strong light source to essentially blind these other cameras. Other methods allow for external policies to be communicated through shared databases [28] or through personal area network (PAN) technologies such as Bluetooth [29–31]. However, whether intrinsic or extrinsic, these sanitization approaches are still primarily focused on post-captured information, which can still pose security and privacy risks, and they have only been applied on the wide use case of visual capturing devices and not on actual MR devices or platforms.

Visual Information Abstraction

Abstraction addresses the earlier issues by reducing or eliminating the necessity of accessing the raw visual feed directly. In the `Recognizers` work, a hierarchical recognizer is inserted as an intermediary input protection layer, which also provides *intrinsic* input access control [32]. It follows the concept of least privilege to application input access—applications are only given the least amount of information necessary to run [33]. The least privilege access control has also been applied to secure user gesture detection. The PRE-POSE gesture core, which is also inserted as an intermediary layer, only sends gesture events to the applications instead of the raw visual feed [34].

The same approach has also been used for providing spatial information while maintaining visual privacy [35] in a room-scale MR environment. Again, these applications do not need to know what the contents on the wall are; it only has to know that there is a surface that can be used for projecting outputs. Another recent work demonstrated how the visual processing and network access of a mobile AR/MR application can be siloed to protect visual information from malicious AR/MR applications [36]. However, most of these works employing abstraction are functionality or data specific and have neither presented or exposed actual risks with 3D MR data nor provided demonstration and evaluation against actual attacks.

`SafeMR`**: Visual Information Access Control** Thus, we designed and developed a proof-of-concept object-level abstraction we call `SafeMR` that can form the basis for providing the necessary visual protection for emerging MR applications [37,38]. It (1) provides visual information protection while (2) reducing visual processing latency by taking advantage of concurrent processing through reusable object-level abstractions. Our system follows the least privilege paradigm where applications are only provided with the minimum amount of information necessary for their intended functionality and/or permitted by the user as illustrated in Fig. 7.8. It shows a cascading and diminishing visual information representation which presents the different levels of privilege and, in turn, the amount of information an application has access to.

`SafeMR` is inserted as an intermediary layer between the trusted device APIs (e.g., ARCore) and the third-party applications to provide information access to visual data via object-level abstractions by detecting the objects and exposing them as abstractions to the applications. Applications' access to the object abstractions and the privilege level is specified by the user privacy preferences. Sample screenshots from our demo application are shown in Fig. 7.9. As shown in Fig. 7.9b, object sensitivity can be specified by toggling the detected objects from a list populated by an initial detection process (seen as the top button on the menu with label "MR DEMO INITIALIZE"). This shows object-level permissions and access control. Likewise, we implemented a "privacy slider" to allow the users to change the privilege levels as defined in Fig. 7.8. Figure 7.9c, d illustrates the use of the slider to set two different privilege levels, i.e., level B and D, respectively.

Data Manipulation and Transformations

Sanitization and abstraction methods primarily focus on providing protection by controlling or blocking the data flow. These methods can potentially be limiting in providing data utility. Others have proposed employing data manipulation or transformation to protect sensitive information.

Table 7.2 Security and privacy properties and their corresponding threats as defined in [10]

	Property	Threat	Definition
↑ *Security-oriented*	Integrity	Tampering	Storage, flow, or process of data in MR is not and cannot be *tampered* or *modified*.
	Non-repudiation	Repudiation	Modification or generation of data, flow, or process *cannot be denied*.
	Availability	Denial of Service	Necessary data, flow, or process for an MR system should be available.
	Authorization	Elevation of Privilege	Actions or processes should be originated from authorized and verifiable entities.
	Authentication	Spoofing	Only the legitimate entities should be allowed to access the MR device or service.
	Identification	Anonymity	All actions should be identified to the corresponding entity.
	Confidentiality	Disclosure of Information	All actions involving sensitive or personal data, flow, or process should remain undisclosed.
Privacy-oriented ↓	Anonymity and Pseudonymity	Identifiability	Entities should be able to remove the identifiable association or relationship to the data stored, flow, or process.
	Unlinkability	Linkability	Any link or relationship of the entity, i.e., user or party, to the data stored, flow, or process as well as with other entities (e.g., data to data, data to flow, and so on) cannot be identified or distinguished.
	Unobservability and Undetectability	Detectability	An entities' existence cannot be ensured or distinguished by an attacker, or an entity can be deemed unobservable or undetectable by an adversary, or the entity cannot be distinguished from randomly generated entities.
	Plausible Deniability	Non-repudiation	An entity should be able to deny that they are the originator of a process, data flow, or data storage.
	Content Awareness	Unawareness	An entity (usually the user) should be aware of all data flows or processes divulged, especially those that are personally identifiable or sensitive.
	Policy and Consent Compliance	Non-compliance	An MR system should follow and provide guarantees that it follows the policies that aim to protect the user's privacy or security.

Encryption-Based Techniques Among these methods are encryption-based techniques, which allow for data queries or computations over encrypted data. Various flavors of encryption have been employed in privacy-preserving image and video processing. For example, HE-SIFT [39] performs bit-reversing and local encryption to the raw image before feature description using SIFT [40] to make dominant and sensitive features recessive. Image feature extraction, description, and matching are all performed in the encrypted domain using near full homomorphism and, thus, have a very slow computation time. Improvements such as Leveled-HE reduces the computation time of HE-SIFT [41]. SECSIFT [42,43] also improved on the computation time of HE-SIFT by instead using an order-preserving encryption. Other improvements utilized big data computation techniques to expedite secure image processing such as the use of a combination of MapReduce and ciphertext-policy attribute-based encryption [44], or the use of Google's Encrypted BigQuery Client for Paillier HE computations [45].

Secure Multi-Party Visual Processing Another cryptographic approach used in image and video processing is secure multi-party computation (SMC) or secret sharing, which allows computation of data from two or more sources or parties without necessarily knowing about the actual data each party has. Figure 7.10 shows a possible SMC setup. A privacy-preserving photo-sharing service has been designed using a two-party secret sharing by "by splitting a photo into a public part, which contains most of the volume (in bytes) of the original, and a secret part which contains most of the original's information" [46]. A virtual cloth try-on service also used secret sharing and two-party SMC [47]: the body measurements of the user is split between the user's mobile device and the server and are both encrypted. The server, which has the clothing information, can compute a 3D model of the user wearing the piece of clothing by combining the body measurement information and the clothing information to generate an encrypted output, which is sent to the user device. The user device decrypts the result and combines it with the local secret to reveal the 3D model of the user "wearing" the piece of clothing. However, like most cryptography-based methods, they are algorithm-specific; thus, every algorithm has to be re-engineered to apply cryptographic protocols on their computations.

Facial de-identification Other techniques have focused on facial de-identification using non-cryptographic image manipulation to achieve k-anonymity for providing identity privacy [48–50]. The succeeding face de-identification work has focused on balancing utility and privacy [51]. Contrarily,

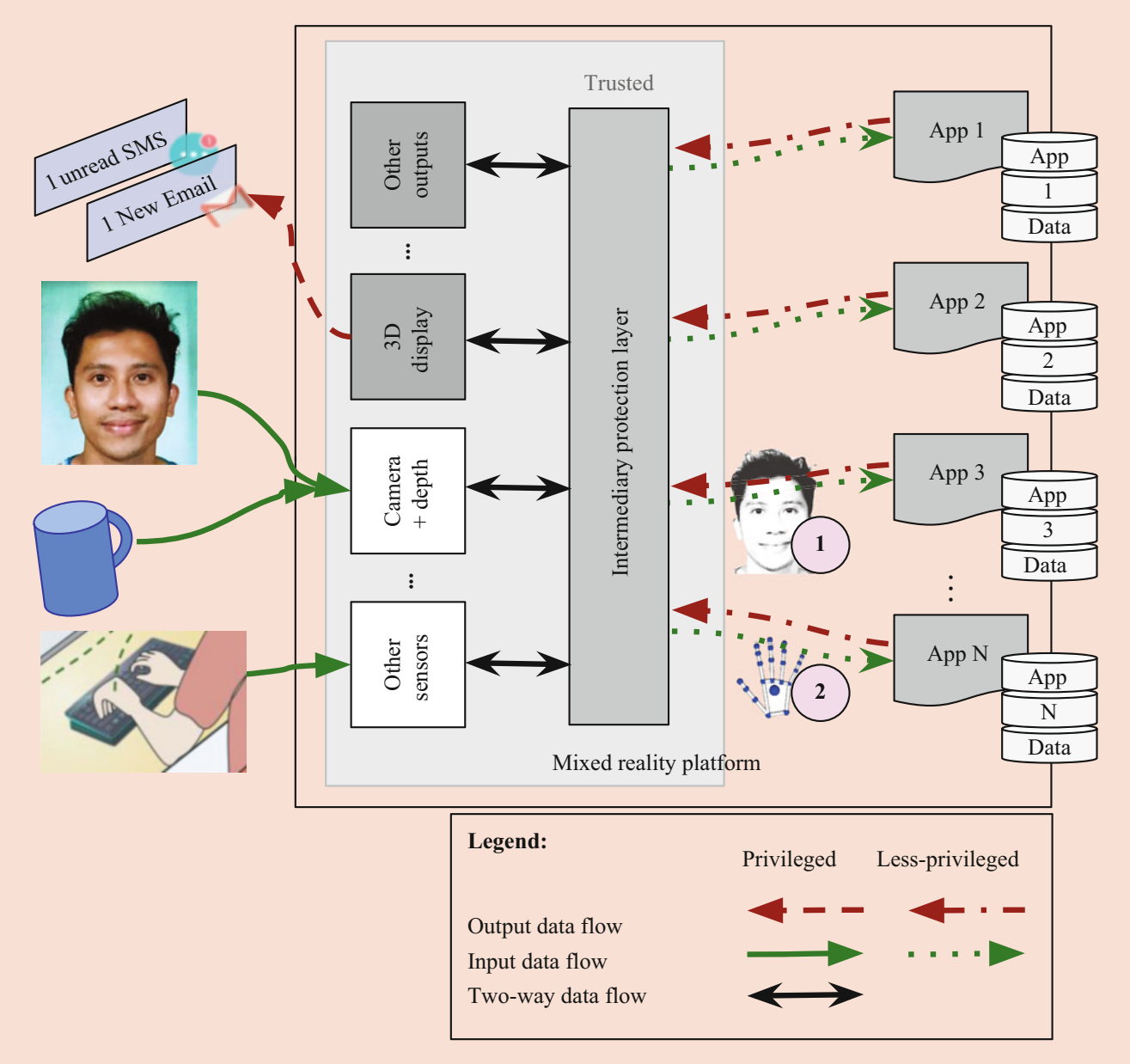

Fig. 7.7 A generic block diagram that shows an inserted ***intermediary protection*** layer between the applications and device resources. Example strategies for input protection are also shown: (1) *information reduction* or *partial sanitization*, e.g., from RGB facial information to facial outline only, or (2) skeletal information instead of raw hand video capture

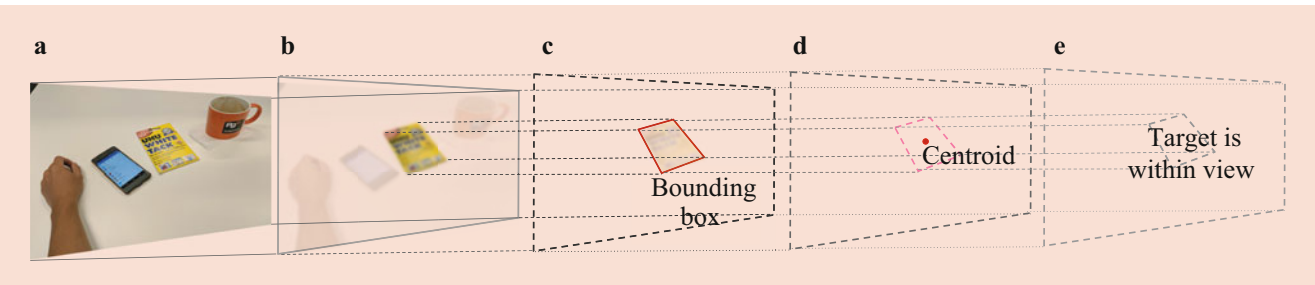

Fig. 7.8 Diminishing information: (**a**) the raw visual capture; (**b**) the target is cropped out but still with complete visual information of the target; (**c**) only the bounding box of the target is exposed; (**d**) only the centroid of the target is exposed; and (**e**) only the binary presence, whether the target is within view or not, is exposed

Fig. 7.9 `SafeMR` demo showing different privilege levels. (**a**) Scene. (**b**) Defining object sensitivity. (**c**) Privilege Level B. (**d**) Privilege Level D

much recent works have leveraged generative adversarial networks for deceiving a potentially adversarial data collector to de-identify faces but ensuring high demographic utility (say, only revealing gender) of the resulting de-identified face [52, 53].

3D Data Attacks and Protection The same manipulation can be extended over 3D spatial data that is utilized in MR systems. Instead of providing complete 3D spatial data, a sanitized or "salted" virtual reconstruction of the physical space can be provided to third-party applications. For example, instead of showing the 3D capture of a table in the scene with all 3D data of the objects on the table, a generalized horizontal platform or surface can be provided. The potentially sensitive objects on the table are thus kept confidential. A tunable parameter provides the balance between sanitization and utility. Using this tunability, similar notions of privacy guarantee to differential privacy and k-anonymity can be provided. However, this approach is yet to be realized, but virtual reconstruction has been used to address delayed alignment issues in AR [54]. This approach can work well with other detection and rendering strategies of sanitization and abstraction as well as in private collaborative interactions. It also opens the possibility to have an active defense strategy where "salted" reconstructions are offered as a honeypot to adversaries. A recent work demonstrated how original scenes from 3D point cloud data can be revealed using machine learning [55]. As a countermeasure, a concurrent work designed privacy-preserving method of pose estimation to counter the scene revelation [56]: 3D "line" clouds are used instead of 3D point clouds during pose estimation to obfuscate 3D structural information; however, this approach only addresses the pose estimation functionality and does not present the viability for surface or object detection, which is necessary for a virtual object to be rendered or "anchored" onto. Thus, it is still necessary for 3D point cloud data to be exposed but with privacy-preserving transformations to hide sensitive content and prevent spatial recognition.

3D Spatial Data Transformations We have investigated the viability of surface-to-plane generalizations as spatial privacy preservation for spatial data captured by the Microsoft HoloLens. Our preliminary work showed evidence on how an adversary can easily infer spaces from captured 3D point cloud data from Microsoft HoloLens and how, even with spatial generalization (i.e., the 3D space is generalized into a set of planes), spatial inference is still possible at a significant success rate [57]. Furthermore, we are also working on deriving a heuristic measure for spatial privacy risk. We refer to spatial privacy as an extension of location privacy; specifically, we pose it as the likelihood of an adversary to identify the space a user is in from the revealed spatial data that is captured by MR devices and platforms like the HoloLens or from ARCore.

Our current work focuses on augmenting the currently inadequate surface-to-plane generalizations with conservative plane releasing (as shown in Fig. 7.11b) as a stronger countermeasure against spatial inference attacks [58]. Our experiments over accumulated data from continuously and

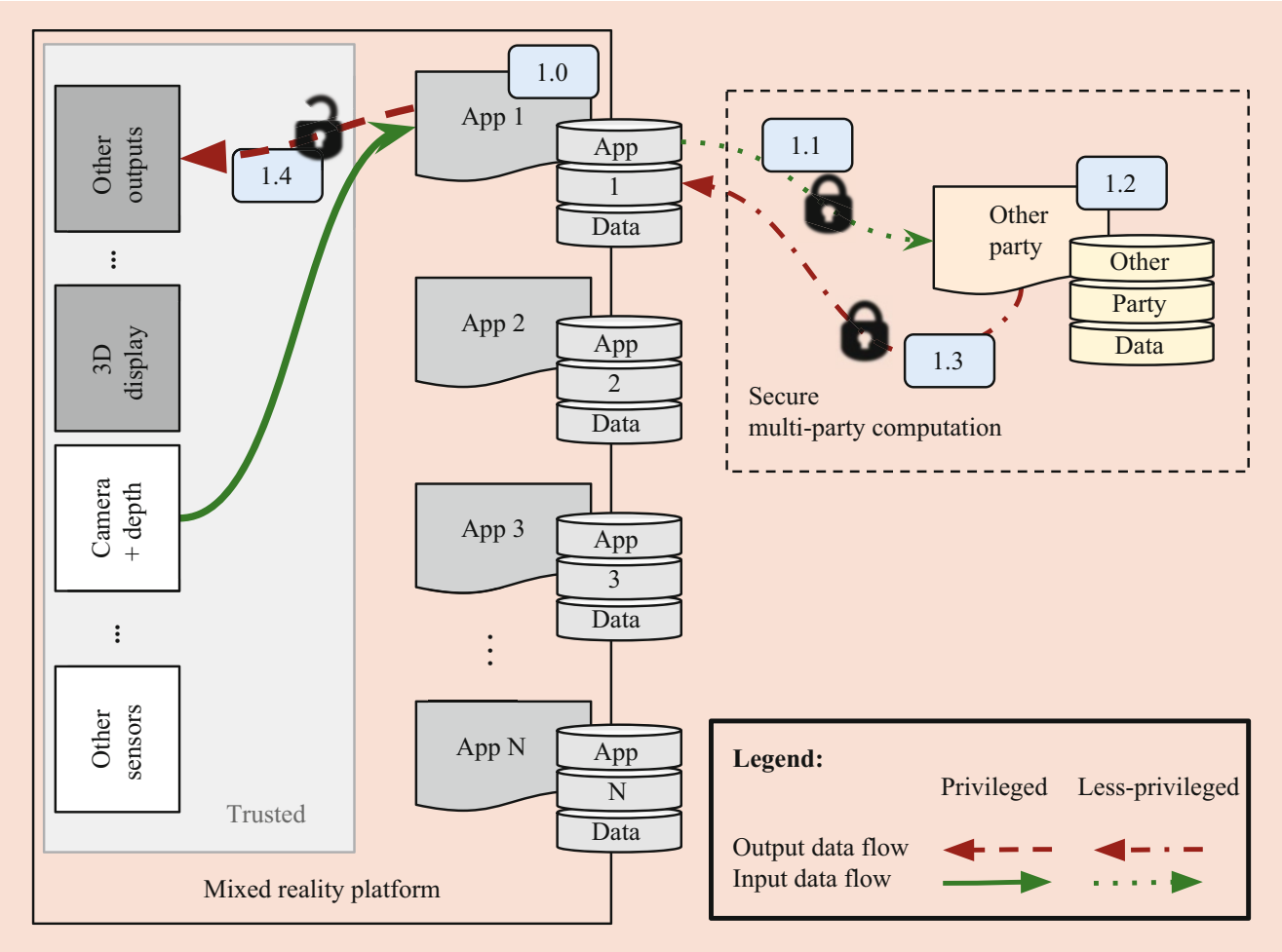

Fig. 7.10 Generic block diagram of a cryptographic technique using *secure multi-party* computation where two or more parties exchange secrets (1.1 and 1.3) to extract combined knowledge (1.2 and 1.4) without the need to divulge or decrypt each other's data share

successively released spatial data showed that we can reveal up to 11 planes and avoid spatial recognition for at least half of the time for sufficiently large revealed spaces, i.e., radius $\leq$ 1.0 meters. And, for the occasions that the adversary correctly recognizes the space, an adversary's guess spatial location can be off by at least 3 meters. Given that plane generalization is already (or can potentially easily be) implemented in most existing MR platforms, thus, perhaps, what remains is the implementation of conservative plane releasing on actual MR platforms as a viable countermeasure against spatial inference attacks.

7.3.2 Output Protection

After capturing and processing data, the resulting outputs of MR applications are sent out to the displays for consumption of the user. Similar to input protection, it is also desirable for applications to only have access and control over their outputs and should not interfere with other outputs or objects. For example, in the smart information hovering over the cup in Fig. 7.6, malicious applications should not be able to modify the sugar-level information. Other adversarial output attacks include clickjacking, i.e., deceives users to "clicking' on sensitive elements through transparent interfaces [9], as well as physiological attacks such as inducing epileptic seizures through a visual trigger [8]. A recent study using immersive VR has demonstrated how to "disorient users, turn [their HMD] camera on without their knowledge, overlay images in their field of vision, and […] control immersed users and move them to a location in physical space without their knowledge." [59].

Output Reliability and User Safety

Despite these output-targeted attacks being brought up as early as 2014 [9], current MR systems still have loose output access control. As a result, adversaries can still potentially *tamper* or *spoof* outputs that can compromise user safety. Despite these output-targeted attacks being brought up as early as 2014 [9], current MR systems still have loose output

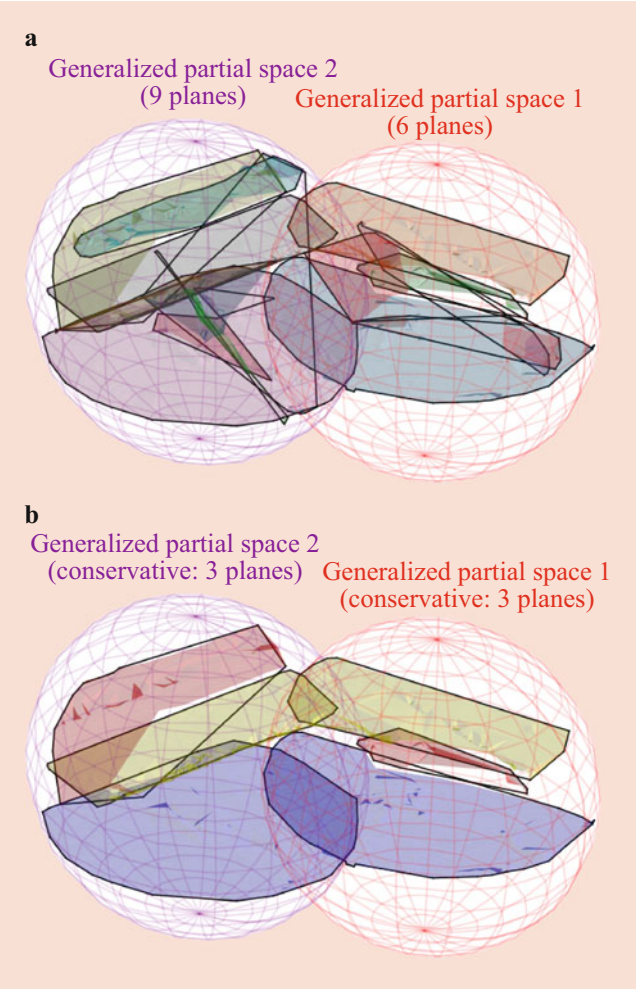

Fig. 7.11 Example of conservative plane releasing. (**a**) Reference generalized partial spaces. (**b**) Conservatively released planes

access control. As a result, adversaries can still potentially tamper or spoof outputs that can compromise user safety. In 2016, an output access control framework with an object-level granularity has been proposed to make output-handling enforcement easier [60]. It can be implemented as an intermediary layer, as in Fig. 7.7, and follows a set of output policies to manage output rendering priority in terms of synthetic object transparency, arrangement, occlusion, and other possible spatial attributes to combat attacks such as clickjacking. In 2017, they followed it up with a design framework [61] called `Arya` for output policy specification and enforcement to ensure policy compliance, integrity, non-repudiation, availability, and authorization. This ensures that correct outputs are always available, an output's originator cannot be denied, and only authorized applications can produce such outputs. A follow-up work focused on mediating rendering conflicts from multiple MR applications [62]. Succeeding work builds up on Arya's weakness when it comes to dynamic and complex environments requiring heterogeneous sources of policies using reinforcement learning [63].

Protecting External Displays

When input and output interfaces are on the same medium or are integrated together such as on touch screens, these interfaces are vulnerable to physical inference threats or visual channel exploits such as shoulder-surfing attacks. MR can be leveraged to provide secrecy and privacy on certain sensitive contexts requiring output confidentiality.Various MR-leveraged strategies include content hiding where a near-eye HMD can deliver secret and private information on public [64]. Most MR eyewear such as the Google Glass can be utilized for this purpose. Other approaches involve the actual hiding of content using optical strategies such as rolling shutter or variable frame rate [65–67]. This technique hides content from human attackers, i.e., shoulder-surfers, but is still vulnerable to machine-aided inference or capture, i.e., setting the capturing device's frame rate to that of the rolling shutter. Other secret display approaches have also used visual cryptographic techniques such as visual secret sharing (VSS) schemes, which allows optical decryption of secrets by overlaying the visual cipher with the visual key. However, these were primarily aimed at printed content [68] and require strict alignment, which is difficult in MR displays. The VSS technique can be relaxed to use standard secret sharing using codes, i.e., barcodes and QR codes. An MR device which has the secret code key can be used to read the publicly viewable code cipher and augment the decrypted content over the cipher. This type of visual cryptography has been applied to both print [69] and electronic displays [70, 71]. These techniques can further be utilized for protecting sensitive content on displays during input capture. Instead of providing privacy protection through, say, post-capture sanitization, the captured ciphers will remain secure as long as the secret shares or keys are kept secure. Thus, even if the ciphers are captured during input sensing, the content stays secure.

7.3.3 Protecting User Interactions

In contrast to current widely adapted technologies like computers and smart phones, MR can enable entirely new and different ways of interacting with the world, with machines, and with other users. Figure 7.12 shows a screenshot from a demonstration video from Microsoft Research on their Holoportation project, which allows virtual teleportation in real time. Consequently, one of the key (yet latent) expectations with these kinds of services and functionalities is how users can have shared space experiences with assurances of security and privacy.

Imbalance of Power from MR Boundaries As early as 1998, concerns on the boundaries between physical and virtual spaces (Fig. 7.6) in MR and on the directionality of these boundaries have been raised [72]. The directionality can influence the balance of power, mutuality, and privacy between users in shared spaces. For example, the boundary (labelled 1) in Fig. 7.13b allows User 2 to receive full information (solid arrow labeled 2) from User 1, while User 1 receives partial information (broken arrow labeled 3) from User 2. The boundary enables an "imbalance of power," which can have potential privacy and ethical effects on the users. For example, early observation work shows territoriality in collaborative tabletop workspaces [73], while a much recent work on multi-user interactions in MR showed the conflicts that can arise, i.e., misuse by multiple actors, apart from the varying degrees of concerns that the user has [19]. Furthermore, this imbalance is not only confined to collaborative but also on non-collaborative shared spaces where, for example, only a subset of the users are using an HMD, such as the Google Glass, while others are not. A great deal of criticism has already been received by Google Glass on its potential violations of privacy.

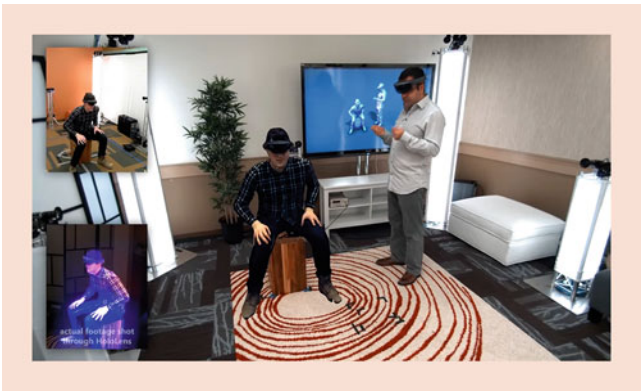

Fig. 7.12 `Holoportation` by Microsoft Research: an example of shared-space service. The person sitting (left) is "holoported" to the room with the person standing (right) using MR technology. Screenshot from https://youtu.be/7d59O6cfaM0. Used with permission from Microsoft

Protecting Collaborative Interactions
Unsurprisingly, the same extrinsic protection is also desired in collaborative interactions to enable user-originated policies and privacy preferences. Early implementations demonstrated how users can change the privacy of virtual objects in a shared virtual environment using privacy lamps and vampire mirrors [74, 75]. (Privacy lamps "emit" a virtual light cone in which users can put objects within the light cone to mark them as private, while *vampire mirrors* are used to determine privacy of objects by showing full reflections of public objects while private objects are either invisible or transparent.) Succeeding work demonstrated the use of hand gestures to signify user privacy preferences [76]. Other developments worked on mediating conflicts in digital workspaces explored the use of multi-user coordination policies [77]. For example, to increase group awareness, they employed cooperative gestures, which requires gesture contributions from more than one user to enforce a single command, such as clearing the entire screen when users do the erase gesture together [78].

Feed-Through Signaling Other developments have also focused on providing feed-through information to deliver signals that would have been available in a shared physical space but is not readily cross-conveyed between remote physical spaces [79]. Feed-through mechanisms were also used to cross-convey user privacy preferences [80]. For example, Fig. 7.13b shows a situation in which User *n* enters the shared space (labelled 4) on the same physical space as User 2, which triggers an alarm (labelled 5) or notification for

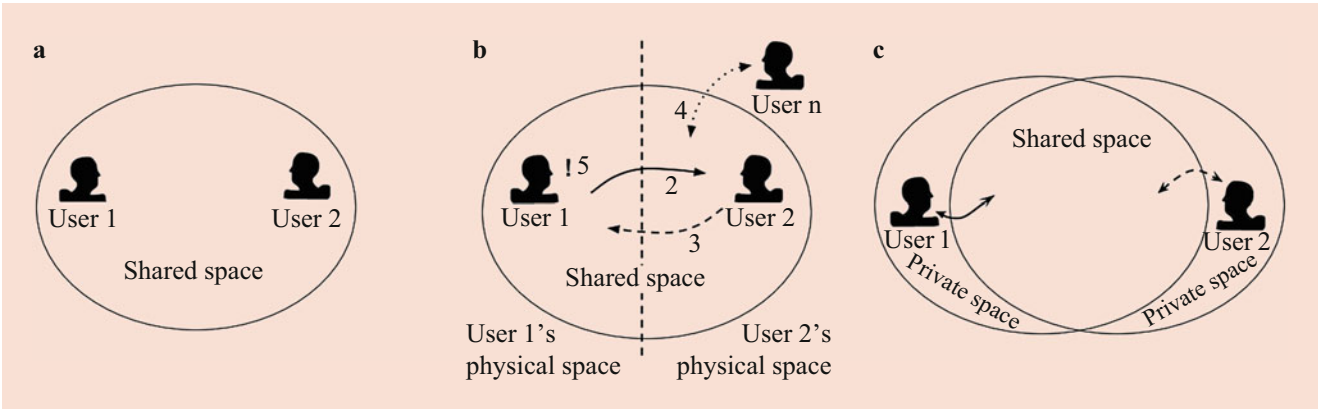

Fig. 7.13 Shared spaces. (**a**) A simplified virtual *shared space* diagram. (**b**) A possible separation in the underlying physical space that creates boundaries between users and devices. (**c**) A collaborative space with a shared space and *private spaces*

User 1. The notification serves as a feed-through signal that crosses over the MR boundary. By informing participants of such information, an imbalance of power can be rebalanced through negotiations. Non-AR feed-through signaling has also been used in a non-shared space context such as the use of wearable bands that lights up in different colors depending on the smartphone activity of the user [81]. However, the pervasive nature of these feed-through mechanisms can still pose security and privacy risks; thus, these mechanisms should be regulated and properly managed. A careful balance between the users' privacy in a shared space and the utility of the space as a communication medium is ought to be sought.

Various strategies also arose from competitive gaming, which demands secrecy and privacy in order to make strategies while performing other tasks in a shared environment. Some of these strategies include Private Interaction Panels (or PIPs) that provides a virtual private region on your gaming console [82] and variable view from see-through AR to full VR [83]. The privacy lamps and mirrors also act as private spaces similar to a PIP. Other PIP-like private regions have been demonstrated on handheld gaming devices [84, 85, 118]. Overall, what rises from these strategies is the utilization of different portions of space as public and private regions where users can actively move objects across the regions to change their privacy.

Protecting Sharing Initialization

Similar to protected external displays, MR can also be leveraged to provide a protected method for securely initializing a collaborative channel. Out-of-band techniques using MR platforms and, thus, leveraging MR capabilities can be employed in secure channel initialization. Such techniques have been demonstrated, including the use of wireless localization paired with facial recognition information for cross-authentication [86], or the use of visual cues for confirming a shared secret using HoloLens [87, 88].

7.3.4 Device Protection

This last category focuses on the actual *physical* MR device and its input and output *interfaces*. This implicitly protects data that is used in the earlier three aspects by ensuring device-level protection. Authentication, authorization, and identifiability are among the most important properties for device protection.

Protecting Device Access

The primary threats to device access are identity spoofing and unauthorized access; thus, all subsequent approaches aim to provide protection against such threats. Currently, password still remains as the most utilized method for authentication [89]. To enhance protection, multi-factor authentication (MFA) is now being adopted, which employs two or more independent methods for authentication. It usually involves the use of the traditional password method coupled with, say, a dynamic key (e.g., one-time password) that can be sent to the user via SMS, email, or voice call. The two-factor variant has been recommended as a security enhancement, particularly for online services like E-mail, cloud storage, e-commerce, banking, and social networks.

To allow users to conveniently wear the MR device (i.e., as a pair of smart glasses), most of the MR device design goal is to achieve the eye-wear form factor. With this, the device is mostly in contact with the user, which allows for various novel authentication methods leveraging physiological signals and other user gestures. Some of these novel strategies include the following: finger and hand gestures using a 3D sensor [90]; head and blinking gestures triggered by visual cues [91]; head movements triggered by an auditory cue [92]; and active physiological signals such as breathing [93], PPG signals [94], and even bone (sound) conduction [95]. Other methods combine two or more modes in a singular method, such as a combination of facial, iris, and periocular information for user authentication [96], and gaze gestures and touch keys [97]. With most HMD MR devices having gaze-tracking and other near-eye sensors, these authentication methods can be easily applied on MR platforms.

Protecting Physical Interfaces

As discussed in the section on external displays (in section "Protecting External Displays"), MR interfaces are vulnerable from malicious inference, which can lead *disclosure* of *input* activity, and/or *output display information*. Currently available MR HMDs project content through see-through lenses. The displayed content on the see-through lenses can leak private information and be observed externally. Visual capturing devices can be used to capture and extract information from the display leakage. Moreover, external input interfaces suffer from the same inference and side-channel attacks.

Various *strategies* have already been discussed in the section on protecting external displays. The same visual cryptographic techniques can be used to protect input/output interfaces [98], or using key scrambling to hide input activity from external inference [99]. Further optical strategies include the use of *polarization* (Fig. 7.14) combined with *narrowband illumination* to maximize display transmission while minimizing leakage [100]. Other strategies use optical reflective properties to only show content at a certain viewing angle [101]. Active camouflaging techniques have also been demonstrated to allow the screens to blend with its surrounding [102]. Both TAPS widgets and the chameleon-inspired camouflaging are physically hiding sensitive objects or information from visual capture. The content-hiding

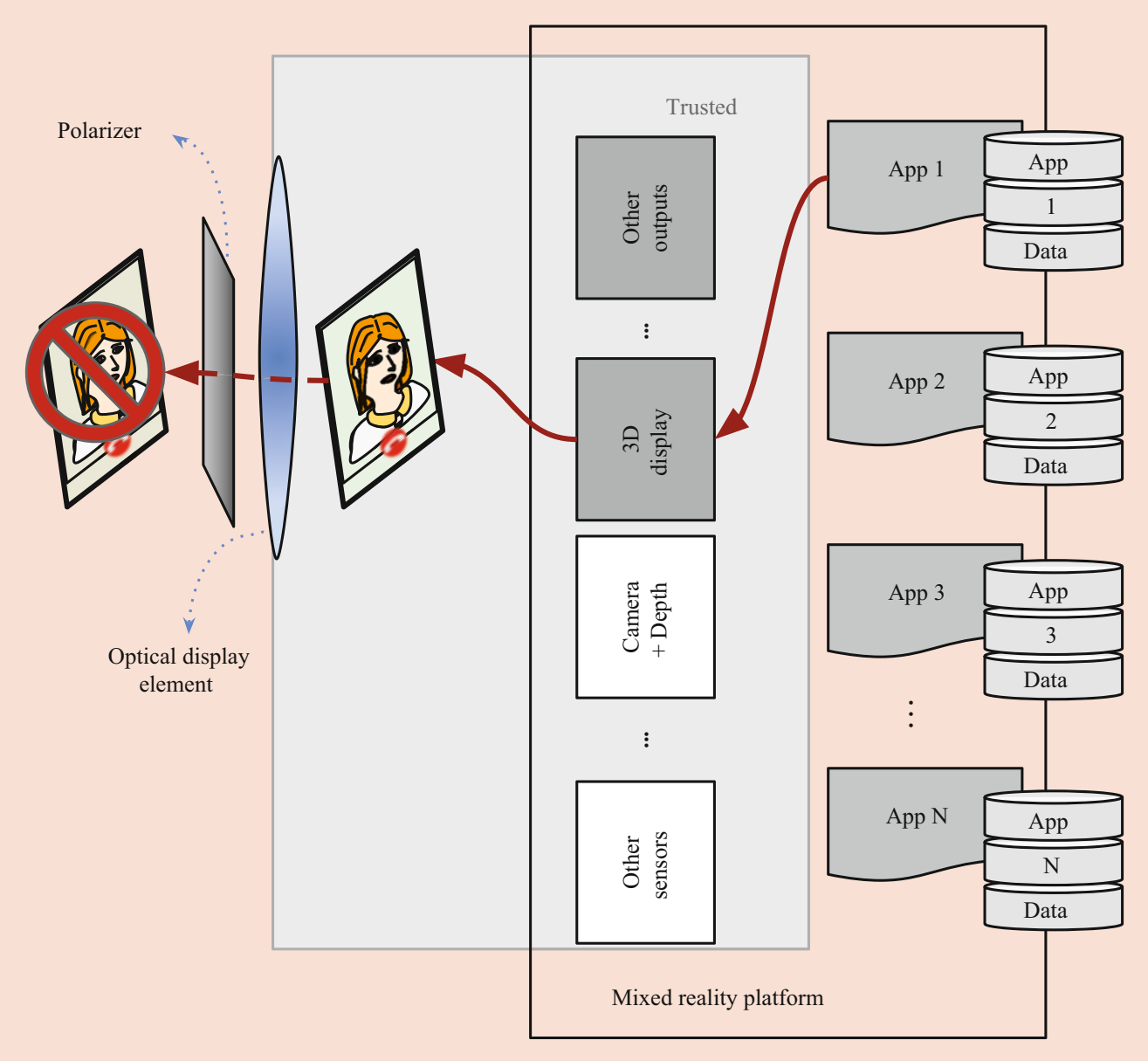

Fig. 7.14 Sample interface protection strategies: inserting a *polarizer* to prevent or block display leakage. All elements to the left of the *optical display element* are considered *vulnerable* to external inference or capture

methods discussed in section "Protecting External Displays" to hide outputs are also optical strategies.

7.3.5 Open Research Challenges

As we have presented a wide understanding of security and privacy in mixed reality, various challenges and opportunities still remain for every aspect. While uptake in mixed reality continues, devices and services will also evolve, leading to new research directions. In this section, we discuss the remaining challenges, potential new opportunities, and future directions.

Remaining Challenges to Input Protection Despite the variety of proposed protection measures, it is still a challenge to determine which objects have to be protected. Specifically, the machine must know what type of inputs or objects the different applications will require and, hence, which sensitive information blended with these inputs need protection. This then requires the necessity for an ontology and taxonomy of objects (including user gestures and inputs) and application requirements, so that specific protection can be applied based on the user-specified sensitivity of the object and as required by the application as well. For example, an MR-painting application may require the detection of different types of brushes, but the machine does not know how to "see" or

detect the brushes. We can use object detection, but we also want to prevent the machine from seeing other sensitive objects. A recent approach has proposed a "a collaborative authorization framework [that integrates] organizations, developers, device manufacturers and users, […] to handle different cases and needs by leveraging attribute-based policies" [103].

Moreover, given the rather specific and heterogeneous challenge, a heterogeneous sensing management framework is also required to allow users to specify and control fine-grained permissions to applications accessing data not just at the sensor level but also at an object level. With this framework, applications must only have access to objects and information they require and must not be able to access the information stream of other applications. Likewise, users should be able to enforce heterogeneous permissions to the different applications. A sensor-level management framework has already been demonstrated in Android [104]. A similar but more fine-grained framework as we have described is necessary for a privacy-aware *near*-future with MR. In conjunction, aside from allowing users to specify the fine-grained permissions, we can also leverage machine learning and artificial intelligence to *dynamically* apply the necessary protection—whether via sanitization, abstraction, or transformation—for both pre-determined and *previously unseen potentially* sensitive objects.

Differently, as MR is now being leveraged in increasing awareness for *dangerous situations* or tasks, say, on manufacturing, it is counter-intuitive to limit the data access of safety and danger warning applications. Thus, it is imperative to employ *heterogeneous access* mechanisms to provide mission-critical applications with full access to environment data. MR device manufacturers (and their developers) can integrate such danger detection and warning systems to the core APIs of their MR device, while other non-critical third-party applications may remain to have minimal access to the environment information.

Remaining Challenges to Output Protection Similar to input protection, an ontological challenge to output protection also arises. This comes from output access control policies being applied also as an intermediary access control layer (see Fig. 7.7) between applications and output interfaces; thus, policies require a heterogeneous mixture of outputs, output channels, and applications. And, to enforce these output control policies, a reference policy framework has to exist through which the protection is applied. A further challenge is the *specification* and *enforcement* of these policies, particularly on who will specify them and how they will be effectively enforced. Furthermore, in the output side, risks and dangers are more imminent because once adversaries have access to the output interfaces, they can actuate malicious response or output, thus the more these output protection strategies are necessitated.

Remaining Challenges to User Interactions The additional dimension of varying user preferences are further compounded by the varying use cases of user interactions. Depending on the context or situation, privacy and security concerns, as well as the degree of concern, can vary. Thus, there is a great deal of subjectivity to determine what is the most effective protection mechanism during sharing or interactions. A recent work has posed a set of security and functionality goals for multi-user MR and demonstrated it using HoloLens [105]. They proposed a design for a sharing control module that can be implemented either as an application- or OS-level interface.

However, a similar ontological challenge also arises as we design and develop these sharing mechanisms, especially as we provide cross-platform-sharing capabilities. Thus, we reiterate that, before everything else, we should probably ask first: "Who or what are we protecting?" Ultimately, the MR platform should be ready to accommodate the various answers to this question, that is, the users (as well as bystanders) should be empowered and be allowed to specify their privacy preferences on these shared MR environments.

Remaining Challenges to Device Protection As MR device and hardware technology research and development continue, various device-level vulnerabilities may arise, which we may have previously been unknown. Thus, we also have to continue to scrutinize the various MR devices that are being released to assess and determine these vulnerabilities with the intention of reducing and mitigating user risks. Nonetheless, some developments on MR (or, generally, wearable) user authentication for device access may include the translation of existing methods from mobile technology, such as fingerprint authentication.

As presented in Sect. 7.3.4, external display protection approaches are particularly helpful in providing security and privacy during certain activities in shared or public spaces due to the secrecy provided, for example, by the near-eye displays, which can perform the decryption and visual augmentation. However, they are mostly applicable to pre-determined information or activities that are known to be sensitive, such as password input or ATM PIN input. Moreover, the visual cryptography or similar approaches are limited by the alignment requirement. Nonetheless, these techniques are still helpful in the contexts they are designed for.

Furthermore, issues on display leakage have also been raised. Given that various display technologies are used for MR devices, various protection methods are also necessary. For example, polarization may not work for certain displays

due to the refractive characteristics of the material used in the MR display.

7.3.6 Future Directions

Aside from the previous remaining challenges on input, output, interaction, and device aspects, we pose the following further challenges and opportunities for future academic endeavors.

Exploring and Extending MR Data Attack Scenarios In Sect. 7.3.1, 3D data protection strategies were presented, which primarily utilize 3D data manipulation to confuse adversaries trying to extract information about the 3D data (e.g., identify the location of the space represented by the 3D data). However, these countermeasures are only as good as the best attack it can defend against. Thus, it is a worthwhile effort to explore improvements on attack scenarios as future work. The current attack scenarios used were based on classifiers using the nearest-neighbor search and deep neural network. Further investigation is required over attack performance of adversaries with strong background knowledge (for example, having access to other user information that can reveal their location) and how these attackers will perform in spatial inference attacks.

Furthermore, there are other platforms and use cases in which 3D data is also used: for example, 3D lidar data used in geo-spatial work, captured by self-driving cars, and, now, by many other applications on recent smartphones. Thus, adversaries from across these various 3D data sources can potentially collude to extract sensitive user information despite current 3D data protection measures.

Risk Analysis of Existing/Future Devices and Platforms As devices and their capabilities continue to evolve, a systematic security and privacy analysis of MR applications, devices, and platforms should still be performed in order to identify other potential and latent risks, particularly on their input capabilities. For example, the scanning capability of current devices, such as the HoloLens, should be further investigated whether it can potentially be used to detect heartbeats or other physiological signals of bystanders or, aside from what we have revealed [57], how these spatial data can be further abused by adversaries.

An integral aspect of device risk analysis is also the risk analysis of the data collected by these devices. In one of our recent work, we presented a measure of risk (in terms of spatial identifiability) using spatial complexity based on stochastic and geometric measurements over the spatial data [106]. Using these measures, we compared the risk of spatial data captured by the Microsoft HoloLens and of Google ARCore (using Google Pixel 2) and showed that Microsoft HoloLens poses more identifiability risks. Similar assessments can be performed on other platforms, such as Apple's ARKit and Oculus VR devices.

Utilization of Other Wearables Majority of past work in security and privacy of MR focused on developing solutions on the primary head-mounted device and its associated peripherals. All indicators are pointing toward the fact that users will wear more than one wearable at all times. For example, smartwatches and smartbands have recently become quite popular among consumers. In the case of security, these devices can be leveraged for continuous or multi-factor authenticators, an alternative channel of communication, environmental or body sensing, etc. In the case of privacy, wearables can be utilized for local processing, alternate non-sensitive form of identifiers, input detection and identification, etc. However, effective integration of such general-purpose wearables into MR sub-system in and around the body will be a challenge for developers when these devices are potentially developed by different vendors. Therefore, extensions of local standards such as UPnP and NSD (Network Service Discovery) would be useful contributions for MR systems.

Protection of Bystander Privacy This is one of the most challenging aspect in the privacy of MR, while it is one of the most impact-full aspect in terms of public acceptance of MR technology. The notion that a person (say, their physical appearance through images) can be inadvertently become part of someone else data collection is a complicated matter to resolve. When Google Glass was first released, there were intense debate about bystander privacy [107]. This has led to banning of Google Glass from a number of public places, which is not the ideal solution. While there is some work in the past [108], practical solutions for bystander privacy are largely an open research challenge.

Edge Computing for MR Security Edge computing has gained significant interest from both academia and industry as a potential solution to latency trade-offs in MR applications [109]. A few investigations on cloud- and edge-assisted platforms for MR mobility were discussed in 7.1.2. However, edge computing, in its current form, will not solve the data ownership and privacy problems. Rather, it could even make them even more acute due to the storage and processing of data in locations/devices that are not under the control of application or service provider.

Similar to MR technology, progresses on these computing paradigms (whether edge, fog, cloud, or their combinations) are still currently being developed. As a consequence, the security and privacy work over these computing paradigms remain to be in silos; however, it is argued that these efforts

need to be in synergy as when we put together various components of, say, an MR mobile environment, novel security and privacy issues arise [110]. Consequently, as both MR and edge computing are currently still being developed, it is opportune to design and develop research platforms or frameworks that allow the co-development of both areas. One potential approach is to dissolve hard boundaries of edge and allow elastic function distribution to different entities that span from user device to traditional cloud depending on the control and ownership of entities. For example, personal laptop, home router, and game controller are more trusted devices compared with edge computing boxes on network base stations. Personal cloud entities like Dropbox are more trusted that cloud storage provided by the MR service. Thus, integration of personal trustworthiness of entities into function orchestration in edge computing will be an interesting future direction.

Shared Standards and Common Ontology Cooperation among developers and manufacturers is required for the use of a standard. This is a common issue with most emerging and currently developing technologies. For example, in the IoT space, there are various existing standards that inadvertently impact the adoption of the technology. Likewise, in MR, there are endeavors in pushing for a shared or open platform particularly for spatial computing, such as the OpenARCloud (https://www.openarcloud.org/oscp).

A common consequence (albeit, mostly, a preliminary one) to standardization is the additional workload and, sometimes, complexity that is loaded to developers in conforming to these standards. An example would be the creation of an ontology of information abstractions in MR. The abstractions limit the information provided to the application, which may require modifications on the processing to provide the same level of service as the original scenario with more information.

Broad Considerations Now, as we desire to be ready for an MR *near*-future, we also ought to consider the various challenges involving the users, developers and device manufacturers, and policymakers.

- **Users.** As the number of users of MR continues to grow, it is imperative that users are made aware of the sensitivity and specificity of the data that is collected from their environment using MR devices. The risks and extent of data collection (not just for 3D MR data) has to be communicated clearly to users. Likewise, users themselves have to take part in the privacy discussion, especially as data protection policies are now being enforced by governments around the world.

  However, the finer-grained (e.g., object-level) user privacy preference specification can extraneously load users. This can become unreasonably taxing, which may defeat the intention of protection. Thus, the perceived utility of the user should also be considered in quantifying the overall quality of experience (QoE).
- **Developers and Device Manufacturers.** Both developers and device manufacturers should also understand the sensitivity of the data that their applications and devices are collecting and handling. For instance, Facebook has recently followed a similar approach unveiling a research-only MR device for the purpose of understanding the breadth and depth of MR challenges before developing and releasing true MR services to everyday users. (Facebook's Project Aria: https://about.fb.com/news/2020/09/announcing-project-aria-a-research-project-on-the-future-of-wearable-ar/) Also, they should be cognizant of the potential reservations that users may have once the users are made aware of the potential risks while using MR services and provide ways for users to either dictate the amount of information they provide or outright prevent collection of information as they desire.
- **Policymakers.** As of 2020, according to the UN Conference on Trade and Development (UNCTAD), 128 out of 194 countries had put legislation that protects user data privacy (https://unctad.org/page/data-protection-and-privacy-legislation-worldwide). Among these is the EU-General Data Protection Regulation (EU-GDPR) whose implementation in May 2018 caused major changes in the privacy policies for most applications worldwide even for non-EU consumers. Despite these significant progresses in legislation and policy enforcement, the actual necessary privacy and security technology remain to either be formulated or developed. Having a shared ontology and taxonomy of the security and privacy terminologies can help in the facilitation, translation, and enforcement of these policies through actual security- and privacy-enhancing technologies. Of course, there are also inherent differences in what is acceptable privacy and security risk that varies between societies and individuals. These variations can potentially complicate the enforcement of the policies and, thus, the implementation of the necessary protection technology.

Nonetheless, it is important to note that these broad challenges are not unique to MR. Likewise with other emerging technologies, we—whether we are from academia, government, or industry—ought to look towards how well-established technologies interact with society in striking a balance between societal and technological progresses.

7.4 Towards Everyday MR Services

MR allows users to interact with machines and each other in a totally different manner: for example, using gestures in the air instead of swiping on screens or tapping on keys. The output of our interactions, also, will no longer be confined within a screen. Instead, outputs will now be mixed with our real-world experience, and soon, we may not be able to tell what is real and what is synthetic. Recently released MR devices such as the Microsoft's HoloLens and the Magic Leap demonstrates what they can do. They allow users to interact with holographic augmentations in a more seamless and direct manner. In prospect, these MR services are likely to be integrated with existing platforms, such as smart phones (which is already happening), wearable devices, and other IoT devices, and will extend, if not enhance, the capabilities of these devices and platforms.

However, (**i**) as MR devices allow for these various novel services, and (**ii**) as novel technologies are integrated to the MR device to provide such services, the security and privacy risks inherent to these services and technologies are then inherited by the MR system. Moreover, the combination of the services and technologies in MR may give rise to novel security and privacy risks.

Summary In this chapter, we have collected, categorized, and reviewed various security and privacy works on MR. Table 7.3 summarizes and presents an overview of all the approaches that have been discussed for every aspect. It also presents a comparison based on which security and privacy properties they address (as defined in Table 7.2). From the summary table, we can see that most of the approaches are focused on input protection. This is understandable as it is more apparent to implement protection at the input side to prevent the capture of sensitive information or, in other input protection approaches, perform post-capture protection before providing the information to the application or service. However, we reiterate that to provide holistic protection, it is also equally important to look into the risks on the other aspects and design protection mechanisms to mitigate these risks. A crucial example is how output-side adversaries can potentially impose harm to users by delivering malicious outputs.

Moreover, the summary table also shows the distribution of the properties addressed by the different approaches. Input protection approaches are privacy-leaning, while the approaches for the other aspects, especially that of device aspect, are security-leaning. This further highlights the need for a synergistic approach to security and privacy in MR. That is, in order to provide protection that addresses most, if not all, of these properties, we need to provide protection for all aspects.

Furthermore, we have highlighted the remaining gaps for every aspect, as well as the broader challenges that MR face. Among the challenges were the necessary risk assessment of other MR devices and platforms, recommendations in the **research methodology** for evaluating performance of protection measures, and the broader considerations when it comes to policy and enforcement. For the latter, the apparent recommendation was the establishment of a shared ontology or taxonomy of security and privacy terminologies and definitions that can (i) facilitate the translation of policy to technology (whether the technology will be applied on the device, edge, or remote cloud or whether it will be), (ii) facilitate in the development of information abstractions for finer-grained policy enforcement, and (iii) allow users to have a common understanding of the risks and the permissions they are giving out.

***Near*-Future with MR** Arguably, ensuring security and privacy for future technologies can ensure the widespread user adoption of these technologies. MR presents a *near* future of new and immersive experiences that will inherently introduce security and privacy risks. Moreover, as MR devices are just starting to ship out commercially, there may still be unknown security and privacy risks.

Figure 7.15, a modified version of Fig. 7.1, shows a system-level recommendation on how to proceed with the provision of a holistic security and privacy protection for MR. Specifically, an intermediary protection layer as seen in Fig. 7.7 is inserted along the MR processing pipeline. Similar to the approaches discussed in 7.3, this proposed layer can provide heterogeneous methods of protection such as abstraction and data transformations. The chosen methods are dictated by the user privacy preferences. Extending the functions of this intermediary layer, we also integrate a means of calculating the risk, say, of user-identifiable information from the data collected by the MR device. Concurrently, a shared ontology can be used to define both the information abstractions and the risks. The same ontology can also be used to design the language of the user privacy preferences.

However, this proposed intermediary layer of protection is ultimately just a paradigm. As we proceed to implement this proposed paradigm, various implementations can arise. It is also important to note that as we proceed with these implementations, novel security and privacy challenges can also arise. Thus, it is important that most subsequent developments be pursued with synergy.

Acknowledgments We would like to thank Kwon Nung Choi for working on the packet analysis shown in Fig. 7.4. We also would like to thank Facebook Reality Labs for partially funding this work through Facebook Research Awards 2020.

Table 7.3 Summary of MR approaches that have been discussed, and which security and privacy properties are addressed by each approach and to what extent

Approach	Integrity	Non-Repudiation	Availability	Authorization	Authentication	Identification	Confidentiality	Anonymity	Unlinkability	Undetectability	Deniability	Awareness	Compliance
Interaction Protection Approaches													
DARKLY [20][a]		✓		✓✓			✓	✓		✓		✓✓	✓
Context-based sanitization [24][a]				✓			✓	✓		✓		✓✓	✓
PLACEAVOIDER [23][b]				✓			✓	✓		✓		✓✓	✓
3D humanoids replace humans [111][a]							✓	✓		✓		✓	✓
OPENFACE/RTFACE [112][b]							✓	✓		✓		✓	✓
Capture-resistant spaces [27][c]				✓			✓	✓		✓			✓
See-through vision [113][a]				✓			✓	✓		✓		✓	✓
World-driven access control [28][a]				✓			✓	✓		✓		✓	✓
iRyp [31][a]				✓			✓	✓		✓		✓	✓
I-PIC [29][b]				✓			✓	✓		✓		✓	✓
PRIVACYCAMERA [30][b]				✓			✓	✓		✓		✓	✓
CARDEA [25][b]				✓			✓	✓		✓		✓	✓
MARKIT [21, 22][b]				✓			✓	✓		✓		✓	✓
PRIVACYEYE [26][b]				✓			✓	✓		✓		✓	✓
PREPOSE [34][a]		✓		✓✓			✓✓			✓			✓
RECOGNIZERS [32][a]		✓		✓✓			✓✓	✓		✓		✓	✓
SAFEMR [37, 38][a]		✓		✓✓			✓✓	✓		✓		✓	✓
AR-SILOS [36][a]		✓		✓✓			✓✓	✓		✓		✓	✓
SEMADROID [104][c]		✓		✓✓			✓			✓		✓	✓
HE-SIFT [41][c]	✓		✓				✓✓			✓	✓		
Leveled HE-SIFT [44][c]	✓		✓				✓✓			✓	✓		

CryptoImg [45][c]	✓						✓✓			✓	✓		
SecSIFT [42,114][c]	✓						✓✓			✓	✓		
P3 [46][c]	✓						✓✓			✓	✓		
Cloth Try-on [47][a]				✓			✓✓	✓	✓	✓✓	✓		
k-anonymous faces [48–50][b]							✓✓	✓✓	✓✓	✓✓	✓		
GAN-based face de-identification [51–53] [b]							✓✓	✓✓	✓✓	✓✓	✓		
Privacy-preserving pose estimation [56][a]							✓✓	✓✓	✓✓	✓✓	✓		
Conservative Plane Releasing [58][a]							✓✓	✓✓	✓✓	✓✓	✓		
SSAC [103][a]	✓	✓	✓	✓✓			✓					✓	✓✓
Output Protection Approaches													
Arya [60–62][a]	✓	✓	✓	✓✓			✓					✓	✓✓
SurroundWeb [33,35][a]				✓			✓	✓		✓✓		✓	✓✓
EyeGuide [64][a]				✓✓			✓✓			✓✓			
VR Codes [65][a]			✓				✓			✓✓			
Psycho-visual modulation [67][a]			✓				✓			✓✓			
Visual cryptography using AR [70][a]							✓✓			✓✓			
Secret messages using AR [71][a]							✓✓			✓✓			
Mobile visual cryptography [115][a]			✓	✓✓			✓	✓					
Interaction Protection Approaches													
Emmie [74,75][a]				✓			✓			✓		✓	✓✓
Kinected Conference [79][a]							✓	✓		✓		✓	✓✓
SecSpace [80][a]		✓	✓			✓	✓					✓✓	✓✓
Candid Interactions [81][c]		✓	✓			✓	✓					✓	✓

(continued)

Table 7.3 (continued)

Approach	Integrity	Non-Repudiation	Availability	Authorization	Authentication	Identification	Confidentiality	Anonymity	Unlinkability	Undetectability	Deniability	Awareness	Compliance
PIP [82, 116][a]				✓			✓			✓		✓	✓
TOUCHSPACE [83][a]				✓			✓			✓		✓	✓
BRAGFISH [84][a]				✓			✓			✓		✓	✓
LooksGoodToMe [86][b]	✓	✓✓	✓	✓	✓✓	✓✓	✓✓					✓	
HOLOPAIR [87], TAPPAIR [88][b]	✓	✓✓	✓	✓	✓✓	✓✓	✓✓					✓	
Device Protection Approaches													
Seamless and secure VR [117][a]					✓✓	✓	✓						
Mid-air authentication gestures [90][b]				✓	✓✓	✓	✓						
Head and blinking gestures [91][b]				✓	✓✓	✓	✓						
HEADBANGER [92][a]				✓	✓✓	✓	✓						
PSKA [94][c]				✓	✓✓	✓	✓						
SKULLCONDUCT [95][b]				✓	✓✓	✓	✓						
Facial multi-modal authentication [96][b]				✓	✓✓	✓	✓						
GAZETOUCHPASS [97][b]				✓	✓✓	✓	✓						
Polarization [100][a]							✓✓			✓✓			
TAPS Widget [101][c]				✓			✓			✓			
Chameleon-like [102][c]				✓			✓			✓			
EYEDECRYPT [98][a]	✓			✓✓		✓	✓✓						
Preventing keystroke inference [99][a]	✓			✓✓			✓						

The extent of each approach was either ✓✓ significantly addressing or ✓ partially addressing the security and privacy properties.
The approaches have been applied to either an [a]MR context, a [b]proto-MR context, or a [c]non-MR context.

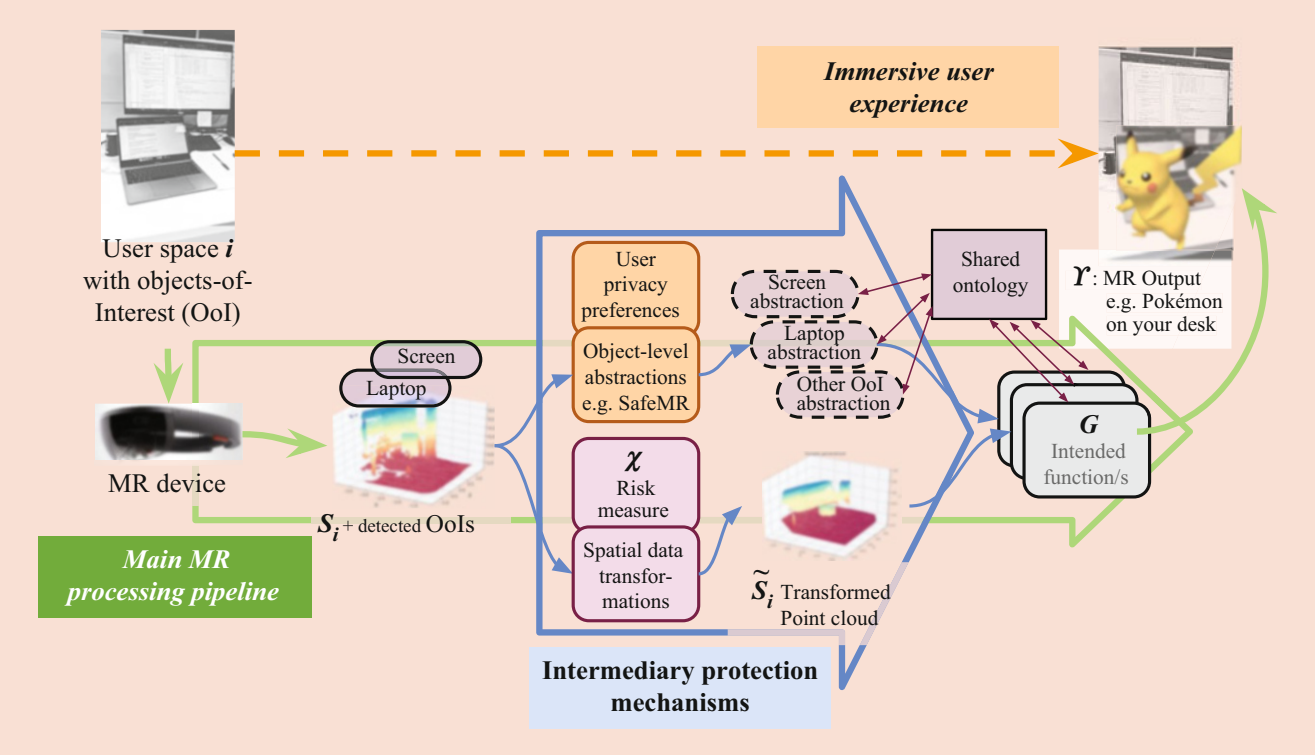

Fig. 7.15 A system diagram showing an *intermediary* layer of protection

References

1. Milgram, P., Kishino, F.: A taxonomy of mixed reality visual displays. IEICE Trans. Inf. Syst. **77**(12), 1321–1329 (1994)
2. Benford, S., Brown, C., Reynard, G., Greenhalgh, C.: Shared spaces: transportation, artificiality, and spatiality (1996)
3. Azuma, R.T.: A survey of augmented reality. Presence Teleoperators Virtual Environ. **6**(4), 355–385 (1997)
4. Azuma, R., Baillot, Y., Behringer, R., Feiner, S., Julier, S., MacIntyre, B.: Recent advances in augmented reality. IEEE Comput. Graphics Appl. **21**(6), 34–47 (2001)
5. Rabbi, I., Ullah, S.: A survey on augmented reality challenges and tracking. Acta Graphica znanstveni časopis za tiskarstvo i grafičke komunikacije **24**(1–2), 29–46 (2013)
6. Heimo, O.I., Kimppa, K.K., Helle, S., Korkalainen, T., Lehtonen, T.: Augmented reality-towards an ethical fantasy? (2014)
7. Friedman, B., Kahn Jr, P.H.: New directions: a value-sensitive design approach to augmented reality (2000)
8. Baldassi, S., Kohno, T., Roesner, F., Tian, M.: Challenges and new directions in augmented reality, computer security, and neuroscience-part 1: Risks to sensation and perception (2018). arXiv preprint arXiv:1806.10557
9. Roesner, F., Kohno, T., Molnar, D.: Security and privacy for augmented reality systems. Commun. ACM **57**(4), 88–96 (2014a)
10. de Guzman, J.A., Thilakarathna, K., Seneviratne, A.: Security and privacy approaches in mixed reality: A literature survey. ACM Comput. Surv. **52**(6), 110:1–110:37 (2019d)
11. Qiao, X., Ren, P., Dustdar, S., Liu, L., Ma, H., Chen, J.: Web ar: A promising future for mobile augmented reality-state of the art, challenges, and insights. Proc. IEEE **107**(4), 651–666 (2019)
12. Villari, M., Fazio, M., Dustdar, S., Rana, O., Ranjan, R.: Osmotic computing: a new paradigm for edge/cloud integration. IEEE Cloud Comput. **3**(6), 76–83 (2016)
13. Zhang, W., Han, B., Hui, P.: Jaguar: Low latency mobile augmented reality with flexible tracking. In: Proceedings of the 26th ACM international conference on Multimedia (2018)
14. Liu, L., Li, H., Gruteser, M.: Edge assisted real-time object detection for mobile augmented reality. The 25th Annual International Conference on Mobile Computing and Networking (MobiCom). ACM, New York (2019)
15. Qiu, H., Ahmad, F., Bai, F., Gruteser, M., Govindan, R.: Avr: Augmented vehicular reality (2018)
16. Liu, L., Zhong, R., Zhang, W., Liu, Y., Zhang, J., Zhang, L., Gruteser, M.: Cutting the cord: Designing a high-quality untethered vr system with low latency remote rendering. In: Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services (2018)
17. Oh, S.J., Benenson, R., Fritz, M., Schiele, B.: Faceless person recognition: Privacy implications in social media. In: European Conference on Computer Vision. Springer, Cham (2016)
18. Acquisti, A.: Privacy in the age of augmented reality. In: Proceedings of the National Academy of Sciences (2011)
19. Lebeck, K., Ruth, K., Kohno, T., Roesner, F.: Towards security and privacy for multi-user augmented reality: foundations with end users. In: Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP). IEEE, New York (2018)
20. Jana, S., Narayanan, A., Shmatikov, V.: A scanner darkly: Protecting user privacy from perceptual applications. In: Proceedings of the 2013 IEEE symposium on security and privacy. IEEE, New York (2013b)

21. Raval, N., Srivastava, A., Lebeck, K., Cox, L., Machanavajjhala, A.: Markit: Privacy markers for protecting visual secrets. In: Proceedings of the 2014 ACM international joint conference on pervasive and ubiquitous computing: Adjunct publication (2014)
22. Raval, N., Srivastava, A., Razeen, A., Lebeck, K., Machanavajjhala, A., Cox, L.P.: What you mark is what apps see. In: Proceedings of the 14th annual international conference on mobile systems, applications, and services (2016)
23. Templeman, R., Korayem, M., Crandall, D.J., Kapadia, A.: Placeavoider: steering first-person cameras away from sensitive spaces. In: NDSS (2014)
24. Zarepour, E., Hosseini, M., Kanhere, S.S., Sowmya, A.: A context-based privacy preserving framework for wearable visual lifeloggers. In: 2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops). IEEE, New York (2016)
25. Shu, J., Zheng, R., Hui, P.: Cardea: Context-aware visual privacy protection from pervasive cameras. arXiv preprint arXiv:1610.00889 (2016)
26. Steil, J., Koelle, M., Heuten, W., Boll, S., Bulling, A.: Privaceye: Privacy-preserving first-person vision using image features and eye movement analysis. CoRR, abs/1801.04457 (2018)
27. Truong, K., Patel, S., Summet, J., Abowd, G.: Preventing camera recording by designing a capture-resistant environment. In: UbiComp 2005: Ubiquitous Computing, pp. 903–903 (2005)
28. Roesner, F., Molnar, D., Moshchuk, A., Kohno, T., Wang, H.J.: World-driven access control for continuous sensing. In: Proceedings of the 2014 ACM SIGSAC conference on computer and communications security (2014b)
29. Aditya, P., Sen, R., Druschel, P., Joon Oh, S., Benenson, R., Fritz, M., Schiele, B., Bhattacharjee, B., Wu, T.T.: I-pic: A platform for privacy-compliant image capture. In: Proceedings of the 14th annual international conference on mobile systems, applications, and services (2016)
30. Li, A., Li, Q., Gao, W.: Privacycamera: Cooperative privacy-aware photographing with mobile phones. In: 2016 13th Annual IEEE international conference on sensing, communication, and networking (SECON). IEEE, New York (2016a)
31. Sun, Y., Chen, S., Zhu, S., Chen, Y.: iRyP: a purely edge-based visual privacy-respecting system for mobile cameras. In: Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (2020)
32. Jana, S., Molnar, D., Moshchuk, A., Dunn, A.M., Livshits, B., Wang, H.J., Ofek, E.: Enabling fine-grained permissions for augmented reality applications with recognizers. In: 22nd USENIX Security Symposium (USENIX Security 13) (2013a)
33. Vilk, J., Molnar, D., Ofek, E., Rossbach, C., Livshits, B., Moshchuk, A., Wang, H.J., Gal, R.: Least privilege rendering in a 3d web browser. In: Microsoft Research Technical Report MSR-TR-2014-25 (2014)
34. Figueiredo, L.S., Livshits, B., Molnar, D., Veanes, M.: Prepose: Privacy, security, and reliability for gesture-based programming. In: 2016 IEEE Symposium on Security and Privacy (SP), pp. 122–137. IEEE, New York (2016)
35. Vilk, J., Molnar, D., Livshits, B., Ofek, E., Rossbach, C., Moshchuk, A., Wang, H.J., Gal, R.: Surroundweb: Mitigating privacy concerns in a 3d web browser. In: 2015 IEEE Symposium on Security and Privacy. IEEE, New York (2015)
36. Jensen, J., Hu, J., Rahmati, A., LiKamWa, R.: Protecting visual information in augmented reality from malicious application developers. In: The 5th ACM Workshop on Wearable Systems and Applications (2019)
37. de Guzman, J.A., Thilakarathna, K., Seneviratne, A.: Safemr: Privacy-aware visual information protection for mobile mixed reality. In: 2019 IEEE 44th Conference on Local Computer Networks (LCN). IEEE, New York (2019c)
38. de Guzman, J.A., Thilakarathna, K., Seneviratne, A.: Demo: Privacy-aware visual information protection for mobile mixed reality. In: 2019 IEEE 44th Conference on Local Computer Networks (LCN). IEEE, New York (2019a)
39. Hsu, C.-Y., Lu, C.-S., Pei, S.-C.: Homomorphic encryption-based secure sift for privacy-preserving feature extraction. In: Media Watermarking, Security, and Forensics III, vol. 7880. International Society for Optics and Photonics, New York (2011)
40. Lowe, D.G.: Distinctive image features from scale-invariant keypoints. Int. J. Comput. Vision **60**(2), 91–110 (2004)
41. Jiang, L., Xu, C., Wang, X., Luo, B., Wang, H.: Secure outsourcing sift: Efficient and privacy-preserving image feature extraction in the encrypted domain. IEEE Trans. Dependable Secure Comput. **17**(1), 179–193 (2017)
42. Qin, Z., Yan, J., Ren, K., Chen, C.W., Wang, C.: Towards efficient privacy-preserving image feature extraction in cloud computing. In: Proceedings of the 22nd ACM international conference on multimedia (2014a)
43. Qin, Z., Yan, J., Ren, K., Chen, C.W., Wang, C.: Secsift: Secure image sift feature extraction in cloud computing. ACM Trans. Multimedia Comput. Commun. Appl. (TOMM) **12**(4s), 65 (2016)
44. Zhang, L., Jung, T., Feng, P., Li, X.-Y., Liu, Y.: Cloud-based privacy preserving image storage, sharing and search. arXiv preprint arXiv:1410.6593 (2014)
45. Ziad, M.T.I., Alanwar, A., Alzantot, M., Srivastava, M.: Cryptoimg: Privacy preserving processing over encrypted images. In: 2016 IEEE Conference on Communications and Network Security (CNS) (2016)
46. Ra, M.-R., Govindan, R., Ortega, A.: P3: Toward privacy-preserving photo sharing. In: 10th USENIX Symposium on Networked Systems Design and Implementation (NSDI 13) (2013)
47. Sekhavat, Y.A.: Privacy preserving cloth try-on using mobile augmented reality. IEEE Trans. Multimedia **19**(5), 1041–1049 (2017)
48. Newton, E.M., Sweeney, L., Malin, B.: Preserving privacy by de-identifying face images. IEEE Trans. Knowl. Data Eng. **17**(2), 232–243 (2005)
49. Gross, R., Sweeney, L., De la Torre, F., Baker, S.: Model-based face de-identification. In: 2006 Conference on computer vision and pattern recognition workshop (CVPRW'06). IEEE, New York (2006)
50. Gross, R., Sweeney, L., de la Torre, F., Baker, S.: Semi-supervised learning of multi-factor models for face de-identification. In: 2008 IEEE Conference on Computer Vision and Pattern Recognition (2008)
51. Du, L., Yi, M., Blasch, E., Ling, H.: Garp-face: Balancing privacy protection and utility preservation in face de-identification. In: IEEE International Joint Conference on Biometrics. IEEE, New York (2014)
52. Brkic, K., Sikiric, I., Hrkac, T., Kalafatic, Z.: I know that person: Generative full body and face de-identification of people in images. In: 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW). IEEE, New York (2017)
53. Wu, Y., Yang, F., Ling, H.: Privacy-protective-gan for face de-identification. arXiv preprint arXiv:1806.08906 (2018)
54. Waegel, K.: [poster] a reconstructive see-through display (2014)
55. Pittaluga, F., Koppal, S.J., Kang, S.B., Sinha, S.N.: Revealing scenes by inverting structure from motion reconstructions. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (2019)
56. Speciale, P., Schonberger, J.L., Kang, S.B., Sinha, S.N., Pollefeys, M.: Privacy preserving image-based localization. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (2019)
57. de Guzman, J.A., Thilakarathna, K., Seneviratne, A.: A first look into privacy leakage in 3d mixed reality data. In: European

Symposium on Research in Computer Security. Springer, Cham (2019b)
58. de Guzman, J.A., Thilakarathna, K., Seneviratne, A.: Conservative plane releasing for spatial privacy protection in mixed reality. arXiv preprint arXiv:2004.08029 (2020)
59. Casey, P., Baggili, I., Yarramreddy, A.: Immersive virtual reality attacks and the human joystick. In: IEEE Transactions on Dependable and Secure Computing (2019)
60. Lebeck, K., Kohno, T., Roesner, F.: How to safely augment reality: Challenges and directions. In: Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications (2016)
61. Lebeck, K., Ruth, K., Kohno, T., Roesner, F.: Securing augmented reality output. In: 2017 IEEE symposium on security and privacy (SP). IEEE, New York (2017)
62. Lebeck, K., Kohno, T., Roesner, F.: Enabling multiple applications to simultaneously augment reality: Challenges and directions. In: Proceedings of the 20th International Workshop on Mobile Computing Systems and Applications (2019)
63. Ahn, S., Gorlatova, M., Naghizadeh, P., Chiang, M., Mittal, P.: Adaptive fog-based output security for augmented reality. In: Proceedings of the 2018 Morning Workshop on Virtual Reality and Augmented Reality Network (2018)
64. Eaddy, M., Blasko, G., Babcock, J., Feiner, S.: My own private kiosk: Privacy-preserving public displays. In: Eighth International Symposium on Wearable Computers, vol. 1. IEEE, New York (2004)
65. Woo, G., Lippman, A., Raskar, R.: Vrcodes: Unobtrusive and active visual codes for interaction by exploiting rolling shutter. In: 2012 IEEE International Symposium on Mixed and Augmented Reality (ISMAR). IEEE, New York (2012)
66. Yerazunis, W., Carbone, M.: Privacy-enhanced displays by time-masking images. In: Australian Conference on Computer-Human Interaction (2002)
67. Lin, P.-Y., You, B., Lu, X.: Video exhibition with adjustable augmented reality system based on temporal psycho-visual modulation. EURASIP J. Image Video Process. **2017**(1), 7 (2017)
68. Chang, J.J.-Y., Li, M.-J., Wang, Y.-C., Juan, J.S.-T.: Two-image encryption by random grids. In: 2010 10th International Symposium on Communications and Information Technologies. IEEE, New York (2010)
69. Simkin, M., Schröder, D., Bulling, A., Fritz, M.: Ubic: Bridging the gap between digital cryptography and the physical world. In: European Symposium on Research in Computer Security. Springer, Cham (2014)
70. Lantz, P., Johansson, B., Hell, M., Smeets, B.: Visual cryptography and obfuscation: A use-case for decrypting and deobfuscating information using augmented reality. In: International Conference on Financial Cryptography and Data Security. Springer, Berlin (2015)
71. Andrabi, S.J., Reiter, M.K., Sturton, C.: Usability of augmented reality for revealing secret messages to users but not their devices. In: Eleventh Symposium On Usable Privacy and Security (SOUPS 2015) (2015)
72. Benford, S., Greenhalgh, C., Reynard, G., Brown, C., Koleva, B.: Understanding and constructing shared spaces with mixed-reality boundaries. ACM Trans. Comput.-Hum. Interact. (TOCHI) **5**(3), 185–223 (1998)
73. Scott, S.D., Carpendale, M.S.T., Inkpen, K.M.: Territoriality in collaborative tabletop workspaces. In: Proceedings of the 2004 ACM conference on Computer supported cooperative work (2004)
74. Butz, A., Beshers, C., Feiner, S.: Of vampire mirrors and privacy lamps: Privacy management in multi-user augmented environments. In: Proceedings of the 11th annual ACM symposium on User interface software and technology (1998)
75. Butz, A., Höllerer, T., Feiner, S., MacIntyre, B., Beshers, C.: Enveloping users and computers in a collaborative 3d augmented reality. In: Proceedings 2nd IEEE and ACM International Workshop on Augmented Reality (IWAR'99). IEEE, New York (1999)
76. Wu, M., Balakrishnan, R.: Multi-finger and whole hand gestural interaction techniques for multi-user tabletop displays. In: Proceedings of the 16th annual ACM symposium on User interface software and technology (2003)
77. Morris, M.R., Cassanego, A., Paepcke, A., Winograd, T., Piper, A.M., Huang, A.: Mediating group dynamics through tabletop interface design. IEEE Comput. Graphics Appl. **26**(5), 65–73 (2006a)
78. Morris, M.R., Huang, A., Paepcke, A., Winograd, T.: Cooperative gestures: multi-user gestural interactions for co-located groupware. In: Proceedings of the SIGCHI conference on Human Factors in computing systems (2006b)
79. DeVincenzi, A., Yao, L., Ishii, H., Raskar, R.: Kinected conference: augmenting video imaging with calibrated depth and audio. In: Proceedings of the ACM 2011 conference on Computer supported cooperative work (2011)
80. Reilly, D., Salimian, M., MacKay, B., Mathiasen, N., Edwards, W.K., Franz, J.: Secspace: prototyping usable privacy and security for mixed reality collaborative environments. In: Proceedings of the 2014 ACM SIGCHI symposium on Engineering interactive computing systems (2014)
81. Ens, B., Grossman, T., Anderson, F., Matejka, J., Fitzmaurice, G.: Candid interaction: Revealing hidden mobile and wearable computing activities. In: Proceedings of the 28th Annual ACM Symposium on User Interface Software and Technology (2015)
82. Szalavári, Z., Eckstein, E., Gervautz, M.: Collaborative gaming in augmented reality. In: Proceedings of the ACM symposium on Virtual reality software and technology (1998)
83. Cheok, A.D., Yang, X., Ying, Z.Z., Billinghurst, M., Kato, H.: Touch-space: Mixed reality game space based on ubiquitous, tangible, and social computing. Personal Ubiquitous Comput. **6**(5–6), 430–442 (2002)
84. Xu, Y., Gandy, M., Deen, S., Schrank, B., Spreen, K., Gorbsky, M., White, T., Barba, E., Radu, I., Bolter, J., et al.: Bragfish: exploring physical and social interaction in co-located handheld augmented reality games. In: Proceedings of the 2008 international conference on advances in computer entertainment technology (2008)
85. Henrysson, A., Billinghurst, M., Ollila, M.: Face to face collaborative ar on mobile phones. In: Fourth ieee and acm international symposium on mixed and augmented reality (ISMAR'05). IEEE, New York (2005)
86. Gaebel, E., Zhang, N., Lou, W., Hou, Y.T.: Looks good to me: Authentication for augmented reality. In: Proceedings of the 6th international workshop on trustworthy embedded devices (2016)
87. Sluganovic, I., Serbec, M., Derek, A., Martinovic, I.: Holopair: Securing shared augmented reality using microsoft hololens. In: Proceedings of the 33rd annual computer security applications conference (2017)
88. Sluganovic, I., Liskij, M., Derek, A., Martinovic, I.: Tap-pair: Using spatial secrets for single-tap device pairing of augmented reality headsets. In: Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy (2020)
89. Dickinson, B.: 5 authentication methods putting passwords to shame (2016)
90. Aslan, I., Uhl, A., Meschtscherjakov, A., Tscheligi, M.: Mid-air authentication gestures: an exploration of authentication based on palm and finger motions. In: Proceedings of the 16th International Conference on Multimodal Interaction (2014)
91. Rogers, C.E., Witt, A.W., Solomon, A.D., Venkatasubramanian, K.K.: An approach for user identification for head-mounted displays. In: Proceedings of the 2015 ACM International Symposium on Wearable Computers (2015)

92. Li, S., Ashok, A., Zhang, Y., Xu, C., Lindqvist, J., Gruteser, M.: Whose move is it anyway? authenticating smart wearable devices using unique head movement patterns. In: 2016 IEEE International Conference on Pervasive Computing and Communications (PerCom). IEEE, New York (2016b)
93. Chauhan, J., Hu, Y., Seneviratne, S., Misra, A., Seneviratne, A., Lee, Y.: Breathprint: Breathing acoustics-based user authentication. In: Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services (2017)
94. Venkatasubramanian, K.K., Banerjee, A., Gupta, S.K.S.: Pska: Usable and secure key agreement scheme for body area networks. IEEE Trans. Inf. Technol. Biomed. **14**(1), 60–68 (2010)
95. Schneegass, S., Oualil, Y., Bulling, A.: Skullconduct: Biometric user identification on eyewear computers using bone conduction through the skull. In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (2016)
96. Raja, K.B., Raghavendra, R., Stokkenes, M., Busch, C.: Multimodal authentication system for smartphones using face, IRIS and periocular. In: International Conference on Biometrics (ICB), pp. 143–150. IEEE, New York (2015)
97. Khamis, M., Alt, F., Hassib, M., von Zezschwitz, E., Hasholzner, R., Bulling, A.: Gazetouchpass: Multimodal authentication using gaze and touch on mobile devices. In: Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems (2016)
98. Forte, A.G., Garay, J.A., Jim, T., Vahlis, Y.: Eyedecrypt—private interactions in plain sight. In: International Conference on Security and Cryptography for Networks. Springer, Cham (2014)
99. Maiti, A., Jadliwala, M., Weber, C.: Preventing shoulder surfing using randomized augmented reality keyboards. In: 2017 IEEE international conference on pervasive computing and communications workshops (PerCom Workshops) (2017)
100. Kohno, T., Kollin, J., Molnar, D., Roesner, F.: Display leakage and transparent wearable displays: Investigation of risk, root causes, and defenses. Technical report (2016)
101. Möllers, M., Borchers, J.: TaPS widgets: interacting with tangible private spaces. In: Proceedings of the ACM International Conference on Interactive Tabletops and Surfaces (2011)
102. Pearson, J., Robinson, S., Jones, M., Joshi, A., Ahire, S., Sahoo, D., Subramanian, S.: Chameleon devices: investigating more secure and discreet mobile interactions via active camouflaging. In: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (2017)
103. Rubio-Medrano, C.E., Jogani, S., Leitner, M., Zhao, Z., Ahn, G.-J.: Effectively enforcing authorization constraints for emerging space-sensitive technologies. In: Proceedings of the 24th ACM Symposium on Access Control Models and Technologies (2019)
104. Xu, Z., Zhu, S.: Semadroid: A privacy-aware sensor management framework for smartphones. In: Proceedings of the 5th ACM Conference on Data and Application Security and Privacy (2015)
105. Ruth, K., Kohno, T., Roesner, F.: Secure multi-user content sharing for augmented reality applications. In: 28th USENIX Security Symposium (USENIX Security 19) (2019)
106. Guzman, J.A.d., Seneviratne, A., Thilakarathna, K.: Unravelling spatial privacy risks of mobile mixed reality data. In: Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, vol. 5(1), pp. 1–26 (2021)
107. Arthur, C.: Google glass security failings may threaten owner's privacy. In: The Guardian: Dostupnona. https://www.theguardian.com/technology/2013/may/01/google-glass-security-privacyrisk [pristupljeno: 08.08. 2019] (2013)
108. Denning, T., Dehlawi, Z., Kohno, T.: In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (2014)
109. Siriwardhana, Y., Porambage, P., Liyanage, M., Ylinattila, M.: A survey on mobile augmented reality with 5g mobile edge computing: Architectures, applications and technical aspects. IEEE Commun. Surv. Tutorials **23**(2), 1160–1192 (2021)
110. Roman, R., Lopez, J., Mambo, M.: Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. Future Gener. Comput. Syst. **78**, 680–698 (2018)
111. Szczuko, P.: Augmented reality for privacy-sensitive visual monitoring. In: International Conference on Multimedia Communications, Services and Security. Springer, Cham (2014)
112. Wang, J., Amos, B., Das, A., Pillai, P., Sadeh, N., Satyanarayanan, M.: A scalable and privacy-aware iot service for live video analytics. In: Proceedings of the 8th ACM on Multimedia Systems Conference (2017)
113. Hayashi, M., Yoshida, R., Kitahara, I., Kameda, Y., Ohta, Y.: An installation of privacy-safe see-through vision. Procedia-Social Behav. Sci. **2**(1), 125–128 (2010)
114. Qin, Z., Yan, J., Ren, K., Chen, C.W., Wang, C., Fu, X.: Privacy-preserving outsourcing of image global feature detection. In: 2014 IEEE global communications conference. IEEE, New York (2014b)
115. Fang, C., Chang, E.-C.: Securing interactive sessions using mobile device through visual channel and visual inspection. In: Proceedings of the 26th Annual Computer Security Applications Conference (2010)
116. Szalavári, Z., Gervautz, M.: The personal interaction panel-a two-handed interface for augmented reality. In: Computer graphics forum, vol. 16(3), pp. C335–C346. Blackwell Publishers Ltd., Oxford (1997)
117. George, C., Khamis, M., von Zezschwitz, E., Burger, M., Schmidt, H., Alt, F., Hussmann, H.: Seamless and secure vr: Adapting and evaluating established authentication systems for virtual reality. In: NDSS (2017)
118. Mulloni, A., Wagner, D., Schmalstieg, D.: Mobility and social interaction as core gameplay elements in multi-player augmented reality. In: Proceedings of the 3rd international conference on Digital Interactive Media in Entertainment and Arts, pp. 472–478. ACM (2008)

Jaybie A. de Guzman has recently concluded his PhD at the UNSW, Sydney, last January 2021. While doing his PhD, he was a research student with the Information Security and Privacy group of CSIRO's Data6. He is currently working on spatial privacy and computer networks and is an Assistant Professor at the Electrical and Electronics Engineering Institute of the University of the Philippines in Diliman, Quezon City, Philippines.

Kanchana Thilakarathna received his PhD from the UNSW, Sydney, in 2015 with the Malcolm Chaikin Prize. He is currently working in cybersecurity and privacy at the University of Sydney. Prior to that, he worked at the information security and privacy group at Data61-CSIRO. He is a recipient of Facebook Research Awards in 2020 and Google Faculty Awards in 2018.

Aruna Seneviratne is currently a Foundation Professor of telecommunications at the University of New South Wales, Australia, where he is the Mahanakorn Chair of telecommunications. He has also worked at many other Universities in Australia, UK, and France and industrial organizations, including Muirhead, Standard Telecommunication Labs, Avaya Labs, and Telecom Australia (Telstra). In addition, he has held visiting appointments at INRIA, France, and has been awarded a number of fellowships, including one at the British Telecom and one at the Telecom Australia Research Labs. His current research interests are in physical analytics: technologies that enable applications to interact intelligently and securely with their environment in real time. Most recently, his team has been working on using these technologies in behavioral biometrics, optimizing the performance of wearables, and verifying the IoT system.