ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

How to Address Privacy Questions Raised by the Expansion of Augmented Reality in Public Spaces

ELLYSSE DICK I DECEMBER 2020

Augmented reality (AR) amplifies some of the most pressing privacy concerns for bystanders in the digital world and combines them in new ways. Policymakers should develop safeguards that allow for shifting perceptions of privacy in public space.

KEY TAKEAWAYS

- The individual privacy concerns from AR are not necessarily unique—smartphones, body cameras, autonomous vehicles, and others raise similar concerns. But AR amplifies and combines existing privacy issues for bystanders.
- Key policy challenges that have defined debates about privacy and technology in the past also apply to AR, including: the expectation of privacy in public space, transparency and choice, government use, child safety, and voluntary practices.
- The potential for AR devices to continuously collect, analyze, and display personal data in real time may challenge existing norms. Adopting these devices widely will require a shift in social and legal definitions of privacy and public space.
- Law enforcement agencies should establish guidelines for their use of AR to address concerns about surveillance and protect Fourth Amendment rights.
- Policymakers should not create unique regulations for AR devices and services, but they should facilitate private sector development of voluntary standards, best practices, and codes of conduct to protect bystanders' privacy.

CONTENTS

INTRODUCTION

When new technologies emerge, they often raise new privacy questions and alter privacy norms, especially when they change how personal information is collected, stored, and processed. These questions can be particularly acute when consumers, businesses, and governments bring these technologies into public spaces where competing priorities, including public safety, civil liberties, and personal privacy, may collide. Augmented reality (AR)—an immersive technology that overlays digitally rendered content on a user's physical environment—is no exception, and the emergence of this technology has the potential to alter both social and legal understandings of privacy and public space.

AR adoption will likely grow substantially in the coming years.[1] While mobile AR (AR applications accessed through a mobile device, such as a smartphone or tablet) has driven the success of this technology to date, wearable AR technologies such as smart glasses are expected to enter the mainstream market in coming years, and other applications such as advanced heads-up displays in vehicles are also on the horizon.[2] As AR and other immersive technologies gain more widespread adoption, there will be two sets of important privacy questions: one set about the collection and use of data about AR users, and one set about the collection and use of data about AR bystanders. This report focuses on the latter set of questions.

Broadly defined, a public space is any area that is generally open to the public. Public spaces include parks, roads, sidewalks, restaurants, stores, beaches, and sports arenas. They are generally available to anyone, but there are rules and norms in place that govern them and individuals' activities within them. For example, laws may allow people to join a protest in a public square, but not allow them to physically or verbally harass passersby. In contrast, private spaces, such as individual homes, personal vehicles, private offices, private clubs, and gated streets, are generally not open to the public.

As a technology becomes more ubiquitous in society, solutions to privacy concerns may emerge as a result of social norms and market responses. AR is positioned to follow this cycle. However, this will only be possible if rules and regulations allow for innovation toward these solutions.

The idea that norms and behaviors vary based on this distinction between public and private spaces underlines the concept of an "expectation of privacy" in the United States, which is tied to Fourth Amendment protections against unreasonable searches. Under this logic, an individual does not have a reasonable expectation of privacy in a public space, where their actions and activities can be observed by anyone. Gathering information in a public space, therefore, generally does not violate anyone's privacy. Of course, in practice, there are some exceptions, such as state and federal laws preventing stalking and harassment, as well as video voyeurism laws that prevent secretly recording people in public bathrooms or store changing rooms. But this basic understanding of privacy and distinctions between public and private spaces informs not only law enforcement and public safety, but also social expectations of privacy. Accordingly, individuals behave and interact differently whenever they are in a space they perceive as public.

Importantly, the expectation of privacy test in law defines "reasonable" as having "a source outside of the Fourth Amendment, either by reference to concepts of real or personal property

law or to understandings that are recognized and permitted by society."[3] This test ties legal parameters of privacy in public space closely to social perceptions of the same, which shift and evolve to accommodate new technologies and changing social norms. In the last century, these parameters have shifted to accommodate widespread adoption of technologies, including handheld cameras, audio and video recordings, telephones, mobile devices, and Internet platforms. Capturing a photo of an individual in a public space has gone from a grave violation of privacy to an accepted practice with select limitations—and communications have evolved from person-to-person or in-person correspondence to enduring and widely accessible posts on social media.

Understanding how new technologies impact the parameters of privacy and public space can help distinguish harmful impacts from this natural evolution. As a technology becomes more ubiquitous in society, solutions to privacy concerns may emerge as a result of social norms and market responses. AR is positioned to follow this cycle. However, this will only be possible if rules and regulations allow for innovation toward these solutions.

Unlike less immersive technologies, AR combines virtual elements with physical space in real time, which effectively alters how users perceive—and interact with—their surroundings. Whether they experience it on a computer screen, mobile device, or wearable headset, AR transports them into a hybrid reality comprising both "real-world" physical elements and digitally rendered content. For example, a homeowner can view digital replicas of furniture in their living room, and a technician can follow visual instructions digitally overlayed on a machine. Simply by looking, AR can allow users to find out more information about the objects, places, and people around them. This hybrid reality is highly personalized, as the digital alterations and additions to physical space can be unique to each user, and depend on the application. While in many cases this information may be completely innocuous, some uses could involve personal information.

Taken individually, the privacy concerns raised by AR are not necessarily new. However, AR amplifies some of the most pressing issues around digital privacy, and combines them in new ways to present novel concerns for bystander privacy in public space. This includes:

- **Continuous data collection:** Some technologies, such as cell phones, smart watches, and fitness trackers, continuously collect data while in use. AR devices similarly have the potential to continuously record audio, video, and other data while in use.
- **Bystander data collection:** Some technologies, such as security cameras, body cameras, and dashcams, collect data about those in the vicinity. Similarly, AR devices have the potential to collect data about users' surroundings, including nearby bystanders.
- **Portable data collection:** Some technologies, such as handheld cameras and audio recorders, are highly portable, which makes it difficult to notify people about the locations where a device might be recording. Some AR devices, such as wearables, are similarly portable.
- **Inconspicuous data collection:** Some technologies, such as hidden cameras, can collect data surreptitiously without any indication that they are recording. AR devices, especially wearable devices, have the potential to collect data without alerting bystanders—and these devices may not be immediately recognizable as recording devices.

- **Rich data collection:** Some technologies, such as smart watches and fitness trackers, collect a wide array of data, such as about an individual's health or location, from sensors. Similarly, some AR devices use a variety of sensors, such as LiDAR sensors to scan 3D objects, or GPS sensors to determine a device's location.
- **Aggregate data collection:** Some technologies, such as license plate readers or facial recognition cameras, collect data that may not present privacy concerns in isolation, but when combined with other data or collected on a very large scale, may reveal sensitive information. AR devices have the potential to collect streams of data that may include information about bystanders, which in the aggregate, may reveal sensitive information.
- **Public data exposure:** Some technologies, such as specialized online databases and interactive maps, make it easier for users to find public information, such as property values, political contributions, sex offenders, or gun permit holders. AR devices have the potential to overlay various public datasets, including from social media, on bystanders.

Consider wearable AR devices such as glasses that provide the user with real-time information about their surroundings. In order to provide this information, the glasses have to continuously record and process data about the objects and individuals their cameras, microphones, and other sensors capture using a combination of on-device and remote processing.[4] For example, these devices may capture, process, amplify, and filter audio from nearby conversations to optimize what the user hears.[5] Widespread adoption of such devices may constrain social and legal parameters of "reasonable expectation of privacy."[6]

This report explores how AR technologies and the hybrid realities they create challenge existing social norms and legal definitions of privacy and the parameters of public space. While AR is hardly the first technology to push these boundaries, this combination of physical and virtual space raises a number of important policy questions that its predecessors did not. By understanding how privacy concerns from AR align with, and diverge from, existing policy questions about technology, privacy, and public space, policymakers can begin to address these impacts before advanced AR technologies gain more widespread adoption by businesses, government, and consumers.

KEY POLICY QUESTIONS ABOUT PRIVACY, TECHNOLOGY, AND PUBLIC SPACE

The rise of AR is not the first time a new technology has clashed with perceptions of reasonable expectations of privacy in public spaces. Debates about the impact of technology on privacy in public space rise and fall with the introduction and widespread adoption of many new technologies.[7] This is understandable: As new innovations change the way individuals interact with each other and the world around them, the parameters of privacy in public space will inevitably shift. Social norms and regulations must then adapt to reflect this new reality and address emerging privacy risks.

Debates around privacy and public space with new technologies tend to address five underlying policy questions:

1. What is a public space, and what is a reasonable expectation of privacy in that space?

2. What are reasonable standards for transparency and choice when using a technology in public spaces?
3. What constitutes acceptable government use of a technology?
4. How should products be developed for children in order to protect their safety and privacy?
5. Can voluntary practices and codes of conduct address privacy concerns?

Redefining Public Space and Reasonable Expectations of Privacy

New technologies can change social as well as legal definitions of public space, and by extension, redefine what constitutes a "reasonable expectation" of privacy. This pattern predates today's digital technologies by at least a century, to when the introduction of the Kodak camera in 1888 made it possible to capture virtually anything, and anyone, on film. Some people were aghast at the privacy implications. One contemporary article in *The Hartford Daily Courant* warned that "the sedate citizen can't indulge in any hilariousness without incurring the risk of being caught in the act and having his photograph passed around among his Sunday school children."[8] As the technology became cheaper, and amateur photography gained popularity at the turn of the century, so did fears about privacy and consent—and with these, a new understanding of what constitutes the "public" and the "private."[9] Within two years, opinions of handheld cameras and amateur photographers rapidly transformed from an interesting new invention to an urgent threat to society—and a new legal framework accompanied this social transformation. Samuel Warren and Louis Brandeis's 1890 *Harvard Law Review* article, simply titled "The Right to Privacy," laid the foundation for legal approaches to privacy in an age of visual media.[10]

The ability to collect massive amounts of data in public spaces, such as from car-mounted or drone-mounted cameras, has raised new questions about privacy.

Despite public fears about a loss of privacy and calls for restrictions on camera use (and indeed some bans at beaches and parks), consumer adoption of this technology continued to increase.[11] By 1905, one-third of American households owned a camera.[12] Ultimately, the ubiquity of amateur photography outweighed the backlash, and within 20 years the handheld camera, and the possibility of appearing in others' photos in public settings, became a rarely-challenged reality of everyday life.

This debate resurfaced in the latter half of the 20th century as audio (and later on, video) recording technologies matured and miniaturized, gaining widespread adoption by amateurs, businesses, and governments.[13] Now it was possible to capture not only someone's likeness, but also their movements and private conversations, sometimes without them even knowing. Once again, social norms and policy had to redefine the parameters of reasonable expectations of privacy in public. From recording conversations to catching viral videos on a smartphone or capturing sweeping images with camera-enabled drones or high-resolution cameras on satellites, these devices made it possible to record, and retain, small moments that may otherwise have been lost or forgotten.[14]

The ability to collect massive amounts of data in public spaces, such as from car-mounted or drone-mounted cameras, has raised new questions about privacy. While cameras collect the images in public spaces, such as public streets or airspace where there is usually no reasonable expectation of privacy, they can potentially capture private activities, such as someone parking at or walking out of a doctor's office. This has led to tensions between legal parameters of privacy, which typically allow for such image collection, and social perceptions, wherein some individuals object to this data collection. In these instances, technical solutions may bridge this disconnect. For example, after public concerns emerged about the images captured by Google's Street View, the company introduced face and license plate blurring features, and later introduced a web page on which users could manually request to blur their home or other sensitive images.

Technologies that aggregate large datasets, such as satellite imagery in Google Earth or geolocation data from a personal device, have further complicated the question of a reasonable expectation of privacy in public. When firms aggregate massive amounts of data collected from public spaces, they can reveal new patterns or information that would otherwise be private. This blurs the line between public and private information by positioning data collected in public as a potential privacy threat. Similar concerns about collecting and aggregating information have arisen around transactional data and sensor data gathered in public spaces. For example, smart doorbell cameras can capture information about activities on public streets, and mobile network operators can gather data about users' physical movements as they manage their network operations.

Online public forums such as social media sites have also changed perceptions of public and private interactions, as they facilitate digital interactions that mirror those of physical public space. Users share information in these spaces, whether through text, speech, video, or simply behaviors, which may be digitally or visually observed. For example, in addition to displaying posts for other users to view, social media platforms use both algorithms and human moderators to screen them for inappropriate or violent content. This raises new questions about the nature of public space, and whether virtual spaces from data flows to public online forums should be governed as public space.[15] These spaces are governed by individual privacy policies as well as the laws of the different countries in which they operate. In both private (e.g., privacy policies) and public (e.g., legal requests for information) governance, online public forums remain a public space without a reasonable expectation of privacy for users.

Developing Practices for Transparency and Choice

Transparency and choice practices, whether informal norms or explicit legal requirements, have historically been introduced to address privacy concerns and build public trust in audio, video, and image-capturing (and more recently, data-collecting) technologies by establishing parameters for their use. These practices may include digital or physical signage, verbal notice, or other indicators; mandates for when explicit consent from subjects is necessary; and voluntary or mandatory privacy measures that can be implemented when explicit consent is not possible.

Once again, the foundations of these practices can be traced back to the beginnings of amateur photography. The ability to capture and distribute images of individuals without their permission led to a distinction between taking photographs in public spaces, which falls under First Amendment protections in the United States, and using those images for different purposes.

Following public outcry about the use of an individual's likeness for commercial purposes without their consent, the New York State Legislature introduced Section 50 and Section 51 of the Civil Rights Law in 1903 to require written consent to use a recognizable likeness of a person for commercial purposes.[16] Similar statutes or common law recognitions of this "right to publicity" have since emerged in a majority of U.S. states.

Digital photography from camera-enabled phones made photography, and fears about intrusive and voyeuristic use, even more ubiquitous. They also introduced new forms of notice, such as a digital flash or mimicking the sound of a camera shutter, to prevent surreptitious use of digital cameras. However, with no legal requirement for their use, these mechanisms are relatively easy to circumvent by simply changing user settings. Even if these features are not directly adjustable, third-party apps and other workarounds can effectively disable them, and studies have shown that these signals do not necessarily reduce rates of socially inappropriate use.[17] The proliferation of social media also adds new dimensions to transparency and choice requirements for distribution.

As state and federal lawmakers debate privacy legislation, the question of how to translate existing transparency norms from image- or audio-based recordings to digital data flows is once again defining new parameters of the division between public and private.

During the 1960s, audio surveillance "bugs" caused a public panic as people envisioned mass "snooping" on private conversations. As a result, the Wiretap Act established transparency requirements for recording audio conversations.[18] At the federal level in the United States, at least one party must agree to the recording (one-party consent), but some states require both parties to agree (two-party consent). These requirements prevent audio recording technology from fully eroding private spaces and individual conversations, but also acknowledge that the parameters of public and private space have shifted due to this technology.

Video recording and surveillance practices have adopted similar norms, although legally, video captured in public spaces without audio is treated similarly to still images. While there is no federal notice requirement for video surveillance, several states have introduced notice laws such as consent for installing hidden cameras or only allowing cameras displayed in plain sight. Even when there is no explicit regulation, many businesses and individuals using video surveillance may choose to display the cameras or post a notice. This effectively establishes a norm for privacy in public and private spaces, even though it is not explicitly codified in federal law.

Online platforms and virtual spaces, from social media to listservs to multiplayer video games, are also spaces in which individuals interact with both each other and digital elements. In doing so, individuals reveal information to each other through direct or indirect communication, and to the services they are using through data analytics. Digital information capture is therefore subject to transparency requirements more suitable for digital space. Data privacy laws such as the California Consumer Privacy Act (CCPA) require websites to provide notice to users both that they are collecting their data and the purpose for which they use this data. This adds a new layer to social perceptions of privacy that extends beyond what is immediately observable to include more complex information and data flows. As state and federal lawmakers debate privacy

legislation, the question of how to translate existing transparency norms from image- or audio-based recordings to digital data flows is once again defining new parameters of the division between public and private.

Implementing Restrictions on Government Use and Access

Defining the parameters of public spaces for new technologies also requires new considerations of what government actors can and cannot do in these spaces. As consumer technologies have evolved—and with them, adjacent technologies such as video and audio surveillance, data collection, and geotracking that could be used by law enforcement—so have definitions of legally acceptable use by governments.

This question of reasonable expectation of privacy from government and law enforcement is consistently debated in relation to surveillance and investigations. As the technologies by which law enforcement can gather data have evolved, public perceptions of surveillance have also shifted. For example, wiretapping grew from primarily a tool of private or corporate espionage to a law enforcement and national security mechanism during the Prohibition era in the United States.[19] In 1928, the Supreme Court's ruling in *Olmstead v. United States* established the constitutionality of wiretapping, and with it, the legal parameters of "reasonable expectation" of privacy within physical bounds.[20] But by the latter half of the century, public and legal understandings of acceptable use by governments shifted. Watergate shook public trust, and the Supreme Court ruling in *Katz v. United States* overturned *Olmstead* to extend Fourth Amendment protections to wiretapping.[21]

This evolution is now taking place in the realm of metadata. The Supreme Court's *Carpenter v. United States* ruling in 2018 further expanded legal definitions of public and private space by applying Fourth Amendment protections to cell phone location data. Coming closely after other technology-enabled privacy rulings, including *United States v. Jones* (2012) and *Riley v. California* (2014), which placed cell phone searches and GPS tracking under Fourth Amendment protections, the *Carpenter* decision effectively introduced new legal parameters for reasonable expectations of privacy in a digital world.[22]

While there is certainly legal precedent to define acceptable use by government actors, there are some use cases that are still being debated. For example, proposals to implement police body cameras as an accountability mechanism have gained notable public support and adoption.[23] But the privacy implications of this technology are not yet entirely clear, as discussions about when cameras should be turned on, who can access the footage, and whether they can be used to record First Amendment activities such as protests complicate the parameters of acceptable use.[24] While activities such as protests do occur in public space, the question of whether protesters should have a reasonable expectation of privacy from body-mounted cameras while exercising First Amendment rights muddles the distinction between public and private that has been used to determine acceptable use in other cases.

Addressing Child Safety Concerns

With many new technologies, child safety is a prominent concern—and often a driving force behind regulatory requirements. Unlike adults, children are unable to understand the complex risks associated with different technologies, much less give meaningful consent where it is

required. This leaves child users particularly vulnerable, and their personal information particularly sensitive. Additional measures are often necessary to ensure children are protected from potential harms when using a technology, including risks of physical harm or harassment by other users.

When e-commerce and household Internet use grew exponentially in the late 1990s, Congress introduced the Children's Online Privacy Protection Act of 1998 (COPPA) to regulate collection of personal information from children under 13. Although initially intended to mitigate potential harms by limiting the amount of data gathered about users known to be children, the law has since evolved to include photo, video, and audio files and more stringent requirements for collecting information from and tracking child users on the Internet.

Since its enactment, COPPA has been used as a benchmark for child privacy compliance by Internet technologies from websites to social media and entertainment platforms, and has fundamentally shaped the way new Internet-driven technology providers approach child safety and privacy concerns.[25] This has restricted innovation in child-focused digital services, and left uncertainties about what compliance looks like for new and emerging technologies as technological advancement continues to outpace regulatory reforms.

Adopting Voluntary Practices and Codes of Conduct

The private companies offering emerging technologies are often best positioned to understand and respond to the unique privacy risks of their products or services. From this recognition, voluntary practices or codes of conduct can emerge across the industry. These practices may be wholly implemented by industry leaders, or developed in consultation with other stakeholders in government and civil society. They allow commercial users and providers to adapt new technologies to align with social perceptions of public space rather than simply complying with existing legal parameters.

Voluntary practices often emerge among early adopters of new technologies that may present privacy risks. For example, the Digital Signage Federation recommended a set of industry-wide privacy standards in 2011 that established guidelines for privacy protections, consent, and transparency when using emerging technologies such as facial recognition.[26] These guidelines offer an important framework for navigating the privacy implications of new technologies in the absence of sufficient regulatory guidance. Government agencies have also implemented voluntary notice for facial recognition that establishes norms beyond legal requirements. When U.S. Customs and Border Protection (CBP) deployed its Biometric Entry-Exit Program, which uses facial recognition to confirm travelers' identities at ports of entry, it included posted signs to notify travelers that this technology is in use. Building on the initial rollout of the program, a September 2020 Government Accountability Office (GAO) report offered additional recommendations to provide comprehensive notice in areas where facial recognition technology is active.[27]

Voluntary practices frequently accompany regulation of highly sensitive forms of information, such as that related to child safety. In addition to the parameters set by COPPA, voluntary codes of conduct have helped guide best practices to protect children's safety in spaces where the distinction between public and private is blurred. Many websites' child privacy protection measures such as moderation practices go well beyond the requirements of COPPA, often times

filling in the legal loopholes that could expose children to greater harm online. COPPA also includes a "safe harbor" provision, which certifies third-party self-regulatory guidelines as compliant under the law.[28]

QUESTIONS ABOUT PRIVACY AND PUBLIC SPACE RAISED BY AR

Perceptions of privacy and public space have evolved over time from social acceptance of photography in public to the recognition of digital platforms as public spaces wherein certain information is no longer private. Now, this evolution is reaching a new phase: privacy in hybrid reality. Rather than operating within physical spaces or facilitating digital information flows, AR technologies alter users' perceptions of their physical space by introducing virtual elements directly into their surroundings, while also collecting information about those environments.

The underlying policy questions that have shaped previous debates about technology and privacy in public space also inform understandings of how AR challenges existing parameters. Many of the questions other new technologies have raised also apply to AR. However, the capabilities and potential use cases of AR also introduce new, technology-specific questions to these debates. Because of this, AR innovation is likely to have a significant impact on both social and legal definitions of public space as hybrid realities become increasingly common in everyday life. By understanding where tensions between physical space and virtual elements appear, policymakers can clarify the legal parameters of public space, while product developers can adapt to shifting social perceptions and regulatory environments.

Parameters of Public Space in AR

AR technologies raise new questions about what constitutes a public space. As with previous iterations of this debate, the combination of AR technology and existing social and legal norms is far from seamless. The primary point of tension is in the collision of virtual and physical space, as questions arise about how AR will impact existing understandings of privacy and physical space. However, as AR technologies become more immersive and digital elements more interactive, the emergence of partially or fully virtual spaces also raises questions about what constitutes a public space when there are no physical parameters.

As AR technologies gain more widespread use across industries, the virtual side of AR could become a form of public space in and of itself. This transformation has already occurred in fully digital spaces on the Internet, where online platforms have become "hyperpublic" spaces in which interactions are not only widely observed, but also retained indefinitely.[29] Now, a more immersive virtual (public) space is emerging: one composed of the purely digital elements and interactions immersive technologies such as AR offer. Such a "virtual public space" requires a markedly different perception of public and private space.

Reasonable Expectations of Privacy in Augmented Reality

The fundamental purpose of AR is to alter a user's perception of physical space in order to achieve certain objectives. This could include viewing a digital rendering of an object in a home, highlighting the best route on a road or walking path, or displaying labels and instructions on machinery. To accomplish this, AR applications and devices use sound-detection and object-recognition capabilities to read a user's surroundings for audio or visual indicators. They then

overlay digital elements onto the surrounding area. In doing so, AR devices display a different version of reality that is more information-rich than what users would perceive without AR.

In some cases, these alterations take place in physical spaces that would traditionally be considered public, such as sidewalks, streets, or parks. But in others, they can overlap with or fully enter private physical space, such as homes—or communal spaces where there is an expectation of privacy such as public restrooms. AR not only blurs the line between public and private space, it also poses challenges to existing rules governing public spaces and reasonable expectations of privacy. While other recording technologies from handheld cameras to video surveillance passively capture the space around them, AR gathers and then actively processes information from the sounds and images that it captures. Rather than merely capturing and retaining a recording, AR uses this information to provide relevant outputs for a user. AR is also highly mobile and relatively inconspicuous, whether used through a wearable device or a mobile phone. These qualities make it more difficult to delineate where AR apps or devices do and do not gather data, or easily recognize when they are in use. Combined with the data-processing capabilities of AR, this requires a new understanding of privacy and public space.

Because virtual spaces are navigated and maintained so differently from their physical counterparts, traditional policy approaches to public space privacy protections do not apply.

Just as some people have balked at the possibility of appearing in amateur photographs for over a century—or more recently have complained about people recording and posting information about their activities on social media—some bystanders today likely object to AR devices recording their interactions or activities, even when they occur in public spaces. Take the Google Glass rollout in 2013: Much like the Kodak "fiends" at the dawn of personal photography, "glassholes" were seen as a public nuisance with a disregard for others' privacy. Not only was the design of Google Glass too conspicuous and the price tag too high to prompt widespread consumer adoption, many found the idea of always-on, Internet-connected wearable devices unsettling. Even with a relatively small number of devices in use, the backlash was swift: The Electronic Privacy Information Center argued that the devices invaded "privacy and anonymity [of people captured by the camera] without their consent."[30] One critic even accused Glass wearers of "demanding social interaction on [their] wholly weird and unsettling terms."[31] It would be reasonable to expect that advanced AR devices equipped with additional sensors would elicit similar critiques, and require a shift in social perceptions of acceptable behavior in public space.

Most virtual spaces are also mediated by a third party that operates the online platforms that enable these virtual spaces. Much like social media platforms, AR service providers are often collecting and storing information about communications and other activity in these virtual spaces. For example, Niantic, the company behind the popular AR game Pokémon Go, collects visual data from players to build out virtual maps of public areas.[32] AR platforms may also choose to use recording and storage mechanisms for trust and safety management, similar to Facebook's immersive social platform Horizon, in which the application maintains a recording of the most recent several minutes of activity, which content moderators or safety managers can review as part of an incident report.[33] As a result, these activities are not entirely private.

Because virtual spaces are navigated and maintained so differently from their physical counterparts, traditional policy approaches to public space privacy protections do not apply. However, they also do not require a dedicated subset of laws and regulations. Rather, other policy mechanisms that are better equipped to regulate virtual spaces must be used in their place. For example, digital privacy and data protection laws can dictate how technology providers can use data that users share in privately managed virtual spaces. Similarly, child protection laws can guard against misuse of children's personal data or personally identifiable features that may be shared in these spaces, such as their voices.

Transparency and Choice Requirements for Hybrid Reality

The hybrid nature of AR introduces unique challenges to the concerns other technologies have raised. Perhaps the most evident is in transparency and choice practices. Unlike technologies tied to a specific location, such as security cameras, most AR devices are mobile, which makes it more difficult to notify bystanders that the technology is in use. Transparency and choice also require a level of public understanding of the technology. Particularly in the early stages of AR adoption, many individuals likely do not understand what it means to be recorded by an AR device—confusion that could hold AR innovation back.

The question of how to provide notice that an AR device is in use also depends on the purpose of the technology. For example, Google Glass included audio and video recording functions. When used in public spaces, for example by journalists, notice could be provided by using verbal notifications or other indications the device was recording. While Google offered these features, ultimately the wearer was responsible for complying with state and federal recording laws, namely one- or two-party consent rules.[34] But more immersive AR devices capture audiovisual information for the purpose of processing and delivering virtual outputs back to the wearer. While they may capture images or audio, they can also process those inputs to provide the user with additional information about individuals and objects around them. These considerations may require different parameters of transparency and choice than those used for more traditional audio and video recordings. First, functionality and consumer preference may discourage overly intrusive notifiers such as lights and sounds. A large flashing light on top of a pair of glasses hardly aligns with the sleek appearance and smooth functionality consumers look for in a product. Second, with the data-processing and recording capabilities of advanced AR devices, subjects may not be aware of, or consent to, these additional capabilities.

There is also the question of who is liable for providing adequate notice. With traditional recording technologies, this is typically the user: the journalist informing a subject they are being recorded, or a supermarket posting signs that video surveillance is in use. In contrast, mobile or wearable AR devices transmit information to the user as well as third-party service providers. The user can inform those around them that they are using an AR device through indicators such as flashing lights, or be held responsible for turning the device off in sensitive locations. But it would be unreasonable to expect them to notify bystanders of the data that is being collected and processed about their surroundings, and how it will be used. While a user may understand the fundamental capabilities of a device, it is extremely unlikely they will have complete knowledge about how it works, and such in-depth transparency requirements could deter consumers from using AR technologies at all. Whether and how service providers and data

processors should also provide some form of notice is likely to be a point of concern as AR use becomes more widespread.

Restrictions on Government Use of AR Technology

AR technologies offer many potential use cases for government, from streamlining workforce development to offering more accessible and efficient services.[35] However, AR also presents questions about restrictions on government and law enforcement use, including protecting sensitive information and determining limits on using real-time aggregate information or metadata from AR devices by law enforcement.

AR Use in Government Services and Operations

When considering limitations on use, it is important to consider all potential applications of AR in government. Unlike other recording technologies that may primarily be used for law enforcement, AR has potential uses across government, from workforce development to public services. For example, AR can guide hands-on training with visual instructions and indicators rather than lengthy manuals. It also offers "see what you see" capabilities that allow instructors, support technicians, or other providers to assess situations and communicate with on-the-ground staff or even members of the public more effectively, without requiring a physical presence. In order to safely and effectively use AR in this way, government agencies will have to consider the privacy implications of AR technologies and their obligations under existing privacy rules—and determine whether additional privacy frameworks are necessary for AR-based government services.

AR Use in Law Enforcement

The highly mobile, largely inconspicuous, and data-intensive nature of mobile and wearable AR that complicates transparency and choice practices also complicates its use by law enforcement. Potential law enforcement use ranges from mapping crime scenes to adding real-time information to surveillance footage.[36] This kind of activity requires different limitations than other government uses. With the ability to process information and identify patterns about surroundings in real time, AR may lead to new legal challenges and calls to delineate publicly available or necessary information and reasonable expectations of privacy from surveillance.

In addition to direct use as an investigative tool, law enforcement could use data from individuals' AR devices in criminal investigations, raising concerns similar to those around GPS data or cell phone records. As mobile and wearable AR gain more widespread use, we may see more legal challenges regarding, for example, government access to metadata logs from an individual's AR device or details about what virtual information a user added to or extracted from their physical environment.

Child Protection in AR

It is important to protect children from harm by or from AR. Children may not be able to distinguish the virtual from the physical in hybrid reality as adults do, leaving them particularly vulnerable to exposure to harmful content, bullying, and harassment, and they may expose their own sensitive or personal information to others. While mechanisms are in place to protect children in physical space and on websites and mobile apps, there has been less work on how to protect children in AR.

Fully digital products can offer child-friendly services that do not collect or transmit data from children without parental consent, but AR technologies developed for child-specific uses may require some of this information, such as location, voice recordings, or demographic information in order to function properly.[37] There are many potential use cases that engage children with AR technology, particularly in education and child development. For example, recent child-focused innovations have shown that AR can improve attention management for children with autism and enrich early childhood education.[38] The privacy concerns of always-on recording and processing of AR devices are also multiplied when considering children's privacy. Parents may object to strangers' AR devices recording, collecting, and processing information about their children, even if they are merely bystanders and not direct targets.

These concerns about data in AR are similar to those raised by other digital technologies that process information about children. As the primary legal benchmark for children's privacy online, COPPA's requirements regarding geolocation data, audio, video, and images currently dictate the parameters of what is considered public and private on the internet in relation to children.[39] Efforts to include other data such as biometric information in compliance requirements further restrict what is allowed in this child-focused hybrid space. This may discourage the development of child-focused AR technologies, just as previous implementations have restricted growth of child-oriented websites and applications.[40]

Opportunities for Voluntary Practices and Codes of Conduct in AR Development

As a new and relatively under-studied technology, AR offers significant opportunities for industry actors to contribute solutions to new privacy risks from their technology. Concerns about AR's potential to diminish individual privacy are an important part of their own decision-making and product-development processes. There are already efforts underway to develop AR-specific frameworks and best practices, such as the XR Safety Initiative's Privacy Framework and individual efforts by companies building AR.[41] As AR devices and use cases evolve, so do the technical capabilities and practical approaches to mitigate privacy risks. In addition to practices such as transparency reporting, industry actors may also be best positioned to develop technical mechanisms to maintain privacy in spaces where their products are in use. Measures such as blurring faces or sensitive information are already in place elsewhere, including widespread services such as Google Street View.[42]

Voluntary standards alone are far from a perfect solution. While there is certainly an incentive for companies to preempt negative impacts, industry alone cannot tackle the complex social, legal, and policy implications of widespread AR use. To do this, companies building AR have to engage directly with policymakers, civil society actors, and other stakeholders to develop these voluntary practices and identify areas where legal or policy intervention may be necessary should codes of conduct fail.

RECOMMENDATIONS

As AR use continues to grow across industries, there is no doubt that it will raise new concerns about privacy and public space. However, while the questions are new, the underlying mechanisms are largely unchanged. Many existing privacy rules and practices can be adapted or directly enforced to address the privacy challenges AR poses. Policymakers should approach concerns about privacy in a hybrid reality within the context of these existing frameworks.

1. Allow Existing Laws and Regulations to Address Privacy Concerns in Public Spaces

In order to support innovation in both AR technologies and effective approaches to privacy protections, policymakers should give AR developers the freedom to iterate and test out new products and practices. When considering bystander privacy, they should resist the urge to preemptively target AR with specific regulations based on hypothetical worst-case scenarios. Adhering to this precautionary principle will prematurely limit the wide-reaching potential of AR and inhibit the processes necessary to develop technical measures and best practices to ensure adequate levels of bystander privacy. Rather, policymakers should approach emerging AR technologies and their impact on privacy in public spaces using the innovation principle, which considers the trade-offs between potential risks and evident benefits.[43]

Following this principle, policymakers should not update laws to redefine public spaces for AR at this stage of innovation. The ongoing debates about privacy and public space in the United States form a strong foundation to define the parameters of public space and reasonable expectations of privacy in U.S. law and policy. As a result, many of the concerns raised by AR specifically can be addressed by existing rules and regulations. As AR technologies continue to develop, policymakers should avoid targeting regulations that could inhibit shifts in social perceptions of privacy as consumers and enterprise users navigate trade-offs between existing perceptions of privacy and the solutions AR devices can offer. Existing privacy rules can mitigate the most immediate potential harms from violations of privacy in public space, such as recording audio without consent, capturing and distributing images for commercial purposes without consent, or making voyeuristic, intrusive, or otherwise harassing recordings of individuals in public.

2. Develop Guidelines to Inform Transparency and Choice Measures Protecting Bystander Privacy

The technical capabilities of AR devices combine those of video and audio recording, image capturing, and data collection—meaning the transparency and choice rules and norms of any one technology cannot be applied directly to AR. To address this, policymakers should consider how these various norms apply to AR, and establish guidelines to develop bystander privacy measures for these technologies. This will help AR providers develop products that comply with existing rules and norms, and discourage restrictions on use that unnecessarily single out AR from other recording devices. Understanding how and when the use of AR-enabled devices overlaps with and diverges from existing norms is critical to this effort.

The Department of Commerce should facilitate this process by convening industry stakeholders and civil society to create voluntary guidelines for operation that companies building AR can use to guide their product development. A voluntary set of standards would allow for more contextual guidelines that consider existing rules and norms. These guidelines should explore the range of technical measures available to address concerns about transparency and choice, including:

- **Indicators** to notify bystanders that a device is in use (such as flashing lights or audio notification);
- **Privacy measures** that use technical capabilities to increase privacy protections in the surrounding area (such as blurring faces or windows); and

- **Restrictions** that limit or fully disable an AR device's functions (such as geofencing to restrict use in certain areas).

Companies building AR can use these guidelines to integrate these measures into products where appropriate, and promote a more unified approach to transparency and choice both for users and bystanders. In addition, any guidance from the federal government should identify existing laws and regulations that apply to AR, such as restrictions on audio recordings or image capturing, which AR providers may wish to notifying users about through terms-of-service and in-product notifications.

3. Develop Standardized Approaches to Government AR Procurement and Use

The U.S. government stands to benefit from greater investment in AR. However, federal agencies and law enforcement should adopt strategic approaches to this investment to ensure AR services and operations improve while serving as a net benefit, rather than endangerment, to society.

AR Use in Government Services and Operations

Due to strong personally identifiable information (PII) and Fourth Amendment legal protections in the United States, it is unlikely that the novelty of AR technology will drastically alter acceptable use by government. For those using government services that utilize AR, existing privacy protections, including the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), can be applied to AR-specific cases. To ensure government AR use falls within these and other existing privacy standards, the General Services Administration should establish government-wide parameters and standardized privacy requirements for AR solutions. These guidelines should consider all potential government use cases, including for training, service provision, and research, as well as future, yet-undiscovered opportunities.

AR Use in Law Enforcement

While AR may challenge "reasonable expectation" tests as a legal mechanism, existing restrictions on government surveillance can also apply to AR. Because the potential for government misuse of AR is similar to that of other audiovisual and network technologies, lawmakers should adapt existing safeguards and best practices to address these concerns. Law enforcement should take preemptive steps to recognize the potential impacts of AR on perceptions of acceptable government use of technology for law enforcement activities.

Using existing rules around other audiovisual and network technologies, the Department of Justice should establish guidelines for AR use by state and local law enforcement in investigations that outline specific use cases and capabilities, including when a warrant is necessary for use, as well as transparency guidelines for when and how to notify the public of AR use by law enforcement officials. In addition, as new AR products for law enforcement become available, they should undergo a pre-deployment review to ensure they meet First and Fourth Amendment protection standards. Such assessments should be conducted by federal officials familiar with existing legal requirements and potential applications. The Facial Recognition Technology Warrant Act introduced in 2019 could serve as a useful model to establish limitations on use, legal requirements for appropriate use, transparency, and approval processes.[44]

4. Ensure Child Protection Measures Encourage Innovation While Mitigating Potential Harms

Protecting children's privacy in hybrid realities is challenging for policymakers and developers alike. However, strict data collection regulations, such as those under COPPA, should not be applied to AR products intended for children, as doing so may risk simply cutting off children from accessing this valuable technology. Child safety standards should instead focus on setting norms to protect against adverse effects, physical harm, and harassment. To better understand where these threats are the strongest, government research bodies including the National Institutes of Health should invest in research on the psychological and physiological effects, and of AR on children and best practices, for child protection measures in hybrid realities. This would not only better inform policymaking in this sensitive area, but also provide companies building AR for children with a stronger knowledge base to ensure their products are safe and secure.

While still safeguarding children from harm through AR technologies, policymakers should also allow space for self-regulatory standards to develop as the technology evolves to ensure the potential benefits to children are not lost in the course of AR innovation. They should also recognize that there is a long history of public hysteria about unsubstantiated negative impacts of new technologies, including television, video games, and social media. The Federal Trade Commission (FTC) and other relevant bodies should make sure existing and proposed data restrictions allow AR and other emerging technologies to collect necessary information to provide engaging services. The FTC should also offer clarification on COPPA compliance standards relating to children's audiovisual, geolocation, and biometric data in AR use cases.

5. Encourage Self-Regulation and Voluntary Codes of Conduct Through a Formal Multi-Stakeholder Process

There are a number of voluntary technical measures, policies, and practices that companies building AR can explore to address concerns about bystander privacy in public spaces. Government agencies should encourage these self-regulatory approaches and integrate them into policy decision-making. A formalized multi-stakeholder approach would help regulators better understand the technological possibilities and limitations of public space privacy protections in AR, allow civil society actors to provide non-technical perspectives on the impacts of AR on privacy, and equip industry leaders with a better understanding of regulatory priorities and constraints.

The National Telecommunications and Information Administration (NTIA) should convene an AR multi-stakeholder process to establish a voluntary code of conduct for companies building AR products and services, which can also serve as a foundation for industry standards while AR innovation is still in its early stages. To address the impacts of AR outlined in this report, the goals of such a working group should include:

- Developing best practices to address concerns about transparency and choice, child safety, and sensitive use cases that are not covered by existing laws;
- Establishing standards to protect bystander privacy through technical measures such as visual indicators, blurring, geofencing, and opt-out functions; and

- Identifying opportunities for government, business, and civil society actors to educate the public about AR technologies, how they collect and process information, and what they are doing to protect bystander privacy.

CONCLUSION

AR offers an exciting vision of a more interconnected, information-rich world. As more consumers utilize AR in their daily lives, and governments and businesses explore the ways in which AR can improve operations and services, individuals increasingly experience the world through the hybrid realities AR creates. If history is any indication, this transition will challenge existing parameters of privacy and public space. When the virtual and the physical world collide, social backlash and legal challenges are all but inevitable.

Policymakers can take steps now to facilitate this transition by mitigating immediate harms while leaving space for AR innovation and voluntary practices to address emerging challenges. AR does not require entirely new regulations—and reactionary or overly restrictive measures could impede technological developments as well as the social evolution necessary to accommodate them. Policymakers should instead focus on identifying existing rules governing privacy and public space that can inform AR use by government, businesses, and consumers. Translating existing rules and best practices into guidelines specific to AR will create a more dynamic framework for determining the parameters of privacy and public space as these technologies continue to develop.

While the underlying policy questions around privacy and public space have remained largely unchanged in over a century, AR raises new questions that shape how individuals interact in both physical and virtual worlds. Recognizing these distinctions in this nascent stage of advanced AR technology is necessary to develop proactive policy approaches for a new era of digital information.

APPENDIX: FRAMEWORK FOR EXAMINING NEW AND EXISTING POLICY QUESTIONS FOR BYSTANDER PRIVACY RAISED BY AR

Policy Questions	Existing Questions	New Questions Raised by AR	Recommendations
(1.a) What is a public space?	• Should there be distinctions between legally and socially defined parameters of public space? • Should some virtual spaces, such as public online forums or social media, be treated as a public space?	• Should a virtual "space" layered on a physical public space be treated like a public space? • Should virtual "spaces" be treated differently when tied to a private space (e.g., in homes)? • Should virtual spaces created for government use be treated as public space?	• Policymakers should refrain from implementing laws that target AR technologies in public spaces.
(1.b) What is a reasonable expectation of privacy in public space?	• Should there be restrictions on what data emerging technologies can capture from public spaces? • Should individuals have a reasonable expectation of privacy when there is pervasive data collection in public spaces? • Should the ability to link together multiple datasets of information gathered in public space be limited to uphold reasonable expectations of privacy?	• Are reasonable expectations of privacy diminished when someone has the ability to aggregate publicly available information to reveal highly contextualized information, which would not otherwise be readily available in real time?	• Allow existing laws and regulations to mitigate the most immediate privacy concerns as AR technologies continue to develop.
(2) What are reasonable standards for notice and consent in public spaces?	• Should parties obtain consent before using digital devices to collect and process data about individuals gathered in public spaces? • Should digital devices alert bystanders when they are actively recording or capturing information? • Should policymakers restrict digital devices from certain sensitive spaces?	• Should AR device users obtain consent from bystanders before allowing a device to gather and process information about them as part of the user's surroundings? • Should AR devices alert bystanders when they are actively recording or capturing information? • Should policymakers restrict AR devices from certain sensitive spaces?	• Establish voluntary standards that encourage the private sector to develop technical mechanisms including data-collection indicators, privacy-enhancing technologies, and measures to restrict use in sensitive areas.

Policy Questions	Existing Questions	New Questions Raised by AR	Recommendations
(3) What constitutes acceptable government use?	• How can government agencies ensure sensitive information about individuals is protected when adopting new technologies for government operations or services? • How can law enforcement use new technologies to improve accuracy and efficiency without violating First and Fourth Amendment rights?	• Should there be restrictions on the aggregate information law enforcement users are permitted to access in real time using AR? • Should it be permissible for law enforcement to use metadata from a private AR device without a warrant?	• Set explicit parameters for AR use by government agencies that comply with existing privacy rules • Establish guidelines for AR use in law enforcement, including limits of reasonable expectation of privacy • Establish a review process for new AR products to inform state, local, and federal law enforcement procurement
(4) How should products protect children's safety and privacy?	• How can new technologies offer beneficial services for children while protecting child users from harms? • Should children receive different or more stringent privacy protections in public spaces than adults?	• To what extent is data collection and transmission necessary to offer AR products for children? • Do existing child protection laws allow for innovation in children's AR products?	• Avoid overregulation of data collection in children's AR • Develop child safety standards that protect against physical harm and harassment • Encourage self-regulation and industry codes of conduct
(5) Can voluntary practices and codes of conduct address privacy concerns?	• How can companies developing new technologies leverage industry knowledge to both preemptively address privacy concerns and fill regulatory gaps? • How can policymakers encourage voluntary practices that protect privacy beyond base levels of legal compliance?	• How can lessons learned from other technologies guide AR innovation?	• Create a multi-stakeholder working group to identify regulatory gaps and develop best practices to address public-space and bystander-privacy concerns

About the Author

Ellysse Dick (@Ellysse_D) is a research fellow in technology and cyber policy at ITIF. Her research focuses on AR/VR innovation and policy including privacy, safety, and accountability. Prior to ITIF, she led communications and outreach for the Women in Public Service Project at the Wilson Center. Dick holds an MA in law and diplomacy from the Fletcher School at Tufts University and a BA in international affairs and German studies from the University of Colorado.

About ITIF

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized as the world's leading science and technology think tank, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

For more information, visit us at www.itif.org.

ENDNOTES

1. *2020 Augmented and Virtual Reality Survey Report,* BoostVC, PerkinsCoie, and the XR Association, March 2020, https://xra.org/wp-content/uploads/2020/07/2020-ar-vr-survey-report-0320-v4.pdf.
2. Tim Merel, "The AR/VR Ecosystem – Are We There Yet?" *VentureBeat,* August 1, 2020, https://venturebeat.com/2020/08/01/the-ar-vr-ecosystem-are-we-there-yet.
3. *Rakas v. Illinois,* 439 U.S. 128 (1978) (U.S. Supreme Court 1978).
4. Franziska Roesner et al., "Augmented Reality: Hard Problems of Law and Policy," Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing (2014), 1283–1288, doi: https://doi.org/10.1145/2638728.2641709.
5. For example, Facebook hopes to introduce enhanced audio in future augmented and virtual reality products. See Lisa Brown Jaloza, "Inside Facebook Reality Labs Research: The Future of Audio," Tech@facebook, September 3, 2020, https://tech.fb.com/inside-facebook-reality-labs-research-the-future-of-audio.
6. Researchers at the University of Washington Tech Policy Lab have noted that widespread use of AR technology could bring both reasonable expectations of privacy and the third-party doctrine under scrutiny as effective legal tools. See Ryan Calo et al., "Augmented Reality: A Technology and Policy Primer," University of Washington School of Law, 2016, https://digitalcommons.law.uw.edu/techlab/1.
7. See Daniel Castro and Alan McQuinn, "The Privacy Panic Cycle: A Guide to Public Fears About New Technologies," Information Technology and Innovation Foundation, September 10, 2015, https://itif.org/publications/2015/09/10/privacy-panic-cycle-guide-public-fears-about-new-technologies.
8. "Beware the Kodak," *The Hartford Daily Courant* (July 28, 1888), https://www.newspapers.com/image/367380225/.
9. Clive Thompson, "The Invention of the 'Snapshot' Changed the Way we View the World," *Smithsonian Magazine,* September 2014, https://www.smithsonianmag.com/innovation/invention-snapshot-changed-way-we-viewed-world-180952435.
10. Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (1890), http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.
11. David Lindsay, "George Eastman," American Experience, n.d., https://www.pbs.org/wgbh/americanexperience/features/george-eastman/.
12. Thompson, "The invention of the 'Snapshot' Changed the Way we View the World."
13. April White, "A Brief History of Wiretapping in America," *Smithsonian Magazine,* April 2018, https://www.smithsonianmag.com/history/brief-history-surveillance-america-180968399.
14. See for example: Ashley Carman, "You Can Keep Recording People in Public, but Don't Capture their Faces," *The Verge,* October 24, 2018, https://www.theverge.com/2018/10/24/18015374/whyd-you-push-that-button-record-stranger-public; Thompson, "The Invention of the 'Snapshot' Changed the Way we View the World."
15. Judith Donath, "Privacy and Public Space," in *The Social Machine,* MIT Press (2020), https://covid-19.mitpress.mit.edu/pub/8icuynaf
16. "New York Right of Publicity Law," Digital Media Law Project, accessed November 5, 2020, http://www.dmlp.org/legal-guide/new-york-right-publicity-law.
17. Mat Smith, "Japan's Noisy iPhone Problem," *Endgadget,* September 30, 2016, https://www.engadget.com/2016-09-30-japans-noisy-iphone-problem.html.
18. 18 U.S. Code § 2511(2)(d)

19. White, "A Brief History of Wiretapping in America."
20. William Lee Adams, "Brief History: Wiretapping," *TIME,* October 11, 2010, http://content.time.com/time/magazine/article/0,9171,2022653,00.html.
21. Thompson, "A Brief History of Wiretapping in America."
22. Louise Matsakis, "The Supreme Court Just Greatly Strengthened Digital Privacy," *WIRED,* June 22, 2018, https://www.wired.com/story/carpenter-v-united-states-supreme-court-digital-privacy.
23. "Police Culture: Public Sees More Benefits than Police from Use of Body Cameras," Pew Research Center, September 24, 2018, https://www.pewsocialtrends.org/2017/01/11/police-culture/psdt_01-11-17-police-06-06-2.
24. Alfred Ng, "Police Body Cameras at Protests Raise Privacy Concerns," *cnet*, June 9, 2020, https://www.cnet.com/news/police-body-cameras-at-protests-raise-privacy-concerns.
25. Makena Kelly and Julia Alexander, "YouTube's New Kids' Content System Has Creators Scrambling," *The Verge*, November 13, 2019, https://www.theverge.com/2019/11/13/20963459/youtube-google-coppa-ftc-fine-settlement-youtubers-new-rules.
26. "Digital Signage Privacy Standards," Digital Signage Federation, February 2011, https://www.digitalsignagefederation.org/wp-content/uploads/2017/02/DSF-Digital-Signage-Privacy-Standards-02-2011-3.pdf.
27. U.S. Government Accountability Office, *Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues,* GAO-20-568, September 2, 2020, https://www.gao.gov/products/GAO-20-568.
28. "COPPA Safe Harbor Program," Federal Trade Commission, https://www.ftc.gov/safe-harbor-program.
29. Donath, "Privacy and Public Space."
30. "Google Glass and Privacy," Electronic Privacy Information Center, accessed November 10, 2020, https://epic.org/privacy/google/glass/default.html.
31. Adrian Chen, "If You Wear Google's New Glasses You Are an Asshole," Gawker, March 13, 2013, https://gawker.com/5990395/if-you-wear-googles-new-glasses-you-are-an-asshole.
32. Lucas Matney, "Niantic to begin collecting 3D visual data from Pokémon GO players," *TechCrunch*, May 26, 2020, https://techcrunch.com/2020/05/26/niantic-to-begin-collecting-3d-visual-data-from-pokemon-go-players.
33. "Horizon Community," Oculus.com, accessed November 10, 2020, https://www.oculus.com/facebook-horizon/community.
34. Kristin Bergman, "Cyborg Journalists: How Google Glass can Change Journalism," Digital Media Law Project, November 19, 2013, http://www.dmlp.org/blog/2013/cyborg-journalists-how-google-glass-can-change-journalism.
35. See for example Ray Briggs et al., "How AR and VR can Enhance Government Services," Deloitte Insights, August 24, 2018, https://www2.deloitte.com/us/en/insights/industry/public-sector/augmented-virtual-reality-government-services.html.
36. Steve Seoane, "How Law Enforcement is Planning on Using Augmented Reality Technology," *GovThink,* September 25, 2019, https://www.govthink.com/2019/09/how-law-enforcement-is-planning-on-using-augmented-reality-technology.
37. Multiple well-established websites for adults, including Snapchat and Facebook Messenger, have attempted to develop COPPA-compliant alternatives for children. In 2013, SnapChat released SnapKidz, a version of the app that allowed younger users to take and edit images, but not send messages. Four years later, Facebook launched Messenger Kids, which lets parents set controls and manage contact lists.

38. See for example: Lizbeth Escobedo et al., "Using Augmented Reality to Help Children with Autism Stay Focused," *IEEE Pervasive Computing* 13, no. 1 (2014), doi: 10.1109/MPRV.2014.19; Igor D.D. Curcio, Anna Dipace, and Anita Norlund, "Virtual Realities and Education," *Research on Education and Media* 8, no. 2 (2015), doi: https://doi.org/10.1515/rem-2016-0019.
39. Federal Trade Commission, "FTC Strengthens Kids' Privacy, Gives Parents Greater Control Over Their Information by Amending Childrens Online Privacy Protection Rule," *ftc.gov*, December 19, 2012, https://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over.
40. See Daniel Castro and Alan McQuinn, "Comments to the Federal Trade Commission on Implementation of the Children's Online Privacy Protection Act," Information Technology and Innovation Foundation, October 11, 2019, https://itif.org/publications/2019/10/11/comments-federal-trade-commission-implementation-childrens-online-privacy.
41. XR Safety Initiative, *The XRSI Privacy Framework Version 1.0,* September 2020, https://xrsi.org/publication/the-xrsi-privacy-framework; for example, Facebook Reality Labs' Project Aria, which is collecting data for future AR products using a wearable research device, included a number of privacy mechanisms. See Nathan White, "Privacy Matters: Project Aria," Facebook Newsroom, September 16, 2020, https://about.fb.com/news/2020/09/privacy-matters-project-aria.
42. "Street View: Policy," Google Maps, accessed September 18, 2020, https://www.google.com/streetview/policy.
43. Daniel Castro and Michael McLaughlin, *Ten Ways the Precautionary Principle Undermines Progress in Artificial Intelligence*, Information Technology and Innovation Foundation, February 4, 2019, https://itif.org/publications/2019/02/04/ten-ways-precautionary-principle-undermines-progress-artificial-intelligence.
44. U.S. Congress, Senate, *Facial Technology Warrant Act of 2019,* S.2878, introduced November 14, 2019, https://www.congress.gov/bill/116th-congress/senate-bill/2878/text.