RISK FRAMEWORK FOR BODY-RELATED DATA IN IMMERSIVE TECHNOLOGIES

DECEMBER 2023

FUTURE OF PRIVACY FORUM

AUTHORED BY

Jameson Spivack
Senior Policy Analyst, Immersive Technologies, Future of Privacy Forum

Daniel Berrick
Policy Counsel, Future of Privacy Forum

EDITORS

Amie Stepanovich
Vice President of U.S. Policy, Future of Privacy Forum

ACKNOWLEDGEMENTS

The authors would like to thank Beth Do, Selin Fidan, Tatiana Rice, Bailey Sanchez, Jordan Wrigley, Maria Badillo, Rob van Eijk, John Verdi, Miranda Lutz, Joan O'Hara, and the many experts whom we consulted for their contributions to this report.

The Future of Privacy Forum (FPF) is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Learn more about FPF by visiting fpf.org.

Risk Framework for Body-Related Data in Immersive Technologies

TABLE OF CONTENTS

TABLE OF CONTENTS *(continued)*

EXECUTIVE SUMMARY

Organizations are increasingly incorporating immersive technologies into their products and services, creating both novel applications and increased risks. This shift typically relies on the collection and use of massive amounts of data about individuals' bodies, and leading organizations developing or deploying immersive tools are adopting risk-based approaches for body-related data practices—approaches that often go beyond legal mandates regarding data handling.

The Future of Privacy Forum's *Risk Framework for Body-Related Data in Immersive Technologies* provides organizations a structure to create appropriate safeguards for the collection, use, and onward transfer of body-related data in immersive technologies. The framework's risk-based approach can be used by organizations to mitigate potential harms and help ensure that data is handled safely and responsibly.

FPF's framework was developed in consultation with privacy experts and is grounded in the experiences of organizations operating in the immersive technology space. It consists of four stages, wherein organizations:

1. **Understand their data practices:** map data practices and specify their purpose.
2. **Evaluate legal obligations:** analyze existing legal obligations and how they may change in the near future.
3. **Identify risks to individuals, communities, and society:** catalog features of data or elements of data practices that create greater risks.
4. **Implement best practices:** operationalize technical, organizational, and legal safeguards to prevent or mitigate the identified risks.

These four steps should be repeated in an ongoing manner to account for changing norms, business practices, and legal requirements.

This framework serves as a straightforward, practical guide for organizations to analyze the unique risks associated with body-related data, particularly in immersive environments, and to institute data practices that earn the public's trust. After consulting this framework, organizations will be able to:

- Evaluate whether their body-related data practices pose privacy risks, namely: whether the data they collect is identifiable, sensitive, prone to sensitive inferences, or biased; and whether their data is used to inform critical decisions, is used fairly by third parties, is retained over time, or is used in ways that individuals expect and understand.
- Implement relevant best practices based on how they handle data, including: data minimization, purpose specification and limitation, meaningful notice and consent, user controls, local and on-device processing and storage, third party management, data integrity, and privacy-enhancing technologies (PETs).

INTRODUCTION

From everyday consumer products like mobile devices and smart home systems, to advanced hardware like extended reality (XR) headsets, technologies are becoming more immersive.[1] These tools are increasingly able to blur the boundaries between the physical and digital worlds, bringing new benefits, as well as risks, to individuals and communities. To maximize the positive impact and minimize the potential harms, organizations must take affirmative steps to ensure that these new capabilities not only comply with the law, but are also built with privacy safeguards appropriate for the sensitivity of the personal data involved.

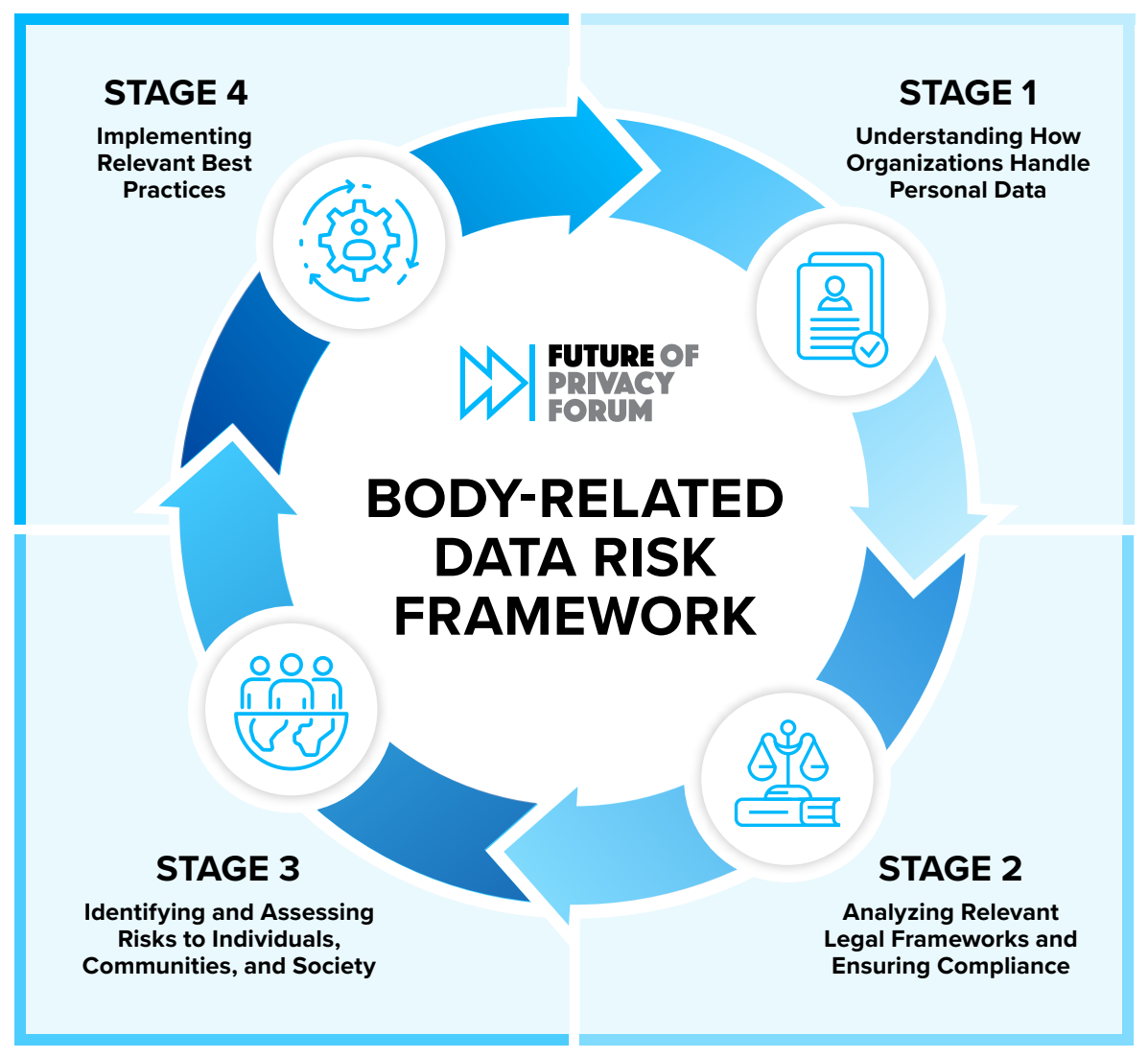
This risk assessment framework serves as a tool for organizations to evaluate their body-related data practices, with a focus on immersive technologies.[2] The emerging immersive technology ecosystem relies on vast amounts of data about people,[3] including their surroundings, interactions, and, critically, their bodies and behaviors. Collecting and aggregating large amounts of body-related data—including bodily responses of which people may not even be aware—can carry significant privacy risks.[4]

Without body-related data, these technologies would be far less immersive, and in some cases, would not function at all.[5] Devices collect data about people's eyes, faces, bodies, and more, which can be further used to infer *more*, and in some cases sensitive information about them.[6] Some of this data is regulated under existing privacy laws. However, many jurisdictions lack privacy laws, and where they do exist the precise contours of these laws are changing as technology evolves, creating uncertainty for organizations that handle this kind of data.

In the absence of consistent, comprehensive legal standards, organizations developing and deploying immersive technologies should go beyond legal mandates to earn public trust by fashioning their data practices around a risk-based approach to body-related data. This framework:

- Assists organizations across the immersive technology ecosystem by providing a starting point from which to further customize their privacy practices.
- Facilitates conversations about body-related data and privacy internally within organizations and externally with relevant stakeholders.
- Educates employees about the purposes and risks of data practices.
- Helps organizations operationalize privacy principles and best practices into the design of their body-related data practices, particularly in the context of immersive technologies.
- Helps organizations understand what legal obligations their body-related data practices might trigger, as well as the privacy and fairness considerations they raise.

This framework is most useful for organizations—including hardware providers, platforms, first-party software developers, and third-party developers—that collect, use, or transfer body-related data to power immersive products or services. It may also be useful for organizations that are exploring the possibility of developing immersive technologies, or that handle body-related data in other contexts.[7] The framework is intended to be implemented on an ongoing basis, responding to changes in technological development, the regulatory environment, and the organization's data practices.



STAGE 1

Understanding How Organizations Handle Personal Data

Organizations that have a comprehensive understanding of their personal data practices will be able to better communicate these practices to their users, directors, shareholders, regulators, potential partners, the general public, and other relevant stakeholders. Doing so is a foundational step to help organizations identify potential privacy risks and implement best practices to mitigate them, enhancing a product's trustworthiness and providing much-needed foresight to experts across the organization.

For organizations to develop a full understanding of their personal data processing, experts across the organization must document what personal data is collected, used, or transferred to others; explain how each data practice serves a purpose; and identify key stakeholders involved in these practices. While this risk framework focuses on body-related data, organizations should understand all of their data practices.

1.1 Create data maps

Data mapping is the process of creating an inventory of all the personal data an organization handles.[8] This includes information such as:

- Personal data the organization collects about individuals.[9]
- What the organization does with this data and why.
- To whom this data is transferred.
- How long this data is kept.

Data mapping is the first step toward developing a comprehensive understanding of an organization's data practices. Tools exist to assist organizations with data mapping,[10] and it is helpful to assign a designated person within an organization—such as a chief privacy officer or data protection officer—to be responsible for completing the data map and keeping it updated as data practices change.

Compliance Tip

Organizations operating in certain jurisdictions likely employ data management tools such as data mapping to comply with privacy laws. For example, the European Union's General Data Protection Regulation (GDPR) requires organizations maintain a record of processing activities, as well as Data Protection Impact Assessments (DPIAs) for high-risk uses, both of which require organizations map out their data flows.[11]

Data Categories and Data Types

Certain kinds of body-related data will be particularly relevant in immersive environments. When developing data maps for immersive technologies, organizations should pay special attention to these data types. Specifically, immersive technologies might collect the following types of body-related data:

FACE AND HEAD
Raw face images, facial geometry, mouth movements, head and neck position and movement[12]

EYE
Raw eye images, gaze, pupillometry, blinks, interpupillary distance, iris and retina measurement, periocular region

VOICE AND SOUNDS
Raw voice recording, visemes (mouth sounds), voice inflections

VITALS
Galvanic skin response, pulse, breathing, blood pressure

HANDS AND LIMBS
Raw hand images, hand position, gestures, fingerprints, palm

BODY
Raw body images, body position, gait, persistent body tracking

NEURAL ACTIVITY
Electroencephalography (EEG), electromyography (EMG)

Resources and best practices for collecting and aggregating large amounts of body-related data remain limited, which may present challenges, particularly for small organizations. Even when organizations institute data mapping, many store data in data lakes (large, unstructured pools of raw data) which can make it difficult to manage data for compliance purposes.[13]

FUTURE OF PRIVACY FORUM

1.2 Document the purpose of each data practice

In order to determine which data practices are necessary, and which may be adjusted, organizations need to know what goal or purpose the data serves. They should also be able to articulate why certain data practices were chosen to accomplish the goal or purpose, and what factors went into the decision-making process.[14]

Organizations might engage in a particular data practice for a variety of purposes: enabling relevant features or products, improving a product's technical performance, facilitating targeted advertising, or customizing a user's experience, to name a few. This documentation will help inform an organization's evaluations of its privacy risks and legal obligations, and generate buy-in from business stakeholders within the organization by linking their interests to privacy compliance.[15]

In documenting data practices, it is beneficial to be as specific as possible. Organizations can use tools and templates to help articulate the purposes of their data practices, guide product and engineering teams within organizations as they build privacy into the design of products, and move towards data minimization and purpose specification.[16] One such tool is the Input, Use, Value Template (illustrated below). Each data practice should be assessed separately to the extent possible, in order to provide a proper basis for assessing each practice's unique risks and implementing relevant privacy safeguards. For organizations operating in certain jurisdictions, such as the EU, specificity about data practices and purposes will also help with legal compliance,[17] helping to dispel reservations about whether the organization's assessment is done at a granular enough level.

Input > Use > Value Template

	INPUT	USE	VALUE TO USER	VALUE TO ORGANIZATION	ALTERNATIVE DATA
Explanation	What is the data input?	How is the data used?	What value does it give the user?	What value does it give the product maker?	Are there alternative data inputs that could be used instead?
Example	Eye tracking	Used to infer items of interest in VR user's field of vision	Personalized content recommendations	Increased user engagement	Like button

The Input, Use, Value Template above is adapted from a resource developed by Meta Trust, Transparency & Control Labs.[18]

1.3 Identify all relevant data stakeholders

Evaluating an organization's legal obligations and privacy risks requires understanding which stakeholders are involved—both as partners in data transfer agreements and as people impacted by the organization's data practices.

1.3.1 Third-party recipients of personal data

Organizations should identify those to whom data is transferred, and those from whom data is received. This includes:

- Actors within an organization—whether departments, teams, projects, or other entities—involved in further distribution of personal data.
- Categories of external actors that receive personal data, including, for example, data processors, third party developers, data brokers, advertisers, researchers, government, or some other type of entity.

Organizations should further identify if any third-party recipients of personal data have commitments or agreements that would require them to further transmit data with other entities in any given circumstance.

1.3.2 Data subjects and other impacted people

Organizations should also identify those who may be impacted by their data practices, including:

- Data subjects for any given tool or service, whose data is most directly impacted. These may be the users of a tool or non-users, about whom data must be collected to enable the tool's primary functionality.
- Bystanders, whose data is implicated by nature of being in the same physical space as a user. These may be individuals with whom the user of a tool directly interacts, or individuals for whom personal data is collected collaterally, either incidentally or by necessity. Bystander data is particularly relevant for XR technologies that collect data about a user's surrounding environment.[19]

Special attention should be paid to individuals and communities whose data may raise additional legal or ethical considerations, such as children and teens, and people from historically marginalized or vulnerable communities. For people in these communities, certain data types, uses, and transfer arrangements may present unique or heightened risks of elevated harm that warrant particular consideration.

Data Practices and Disparate Impact

The impact that any given data practice has will vary by individual and community, often reflecting existing disparities in society.[20] As such, it is important to evaluate a data practice's impacts across demographic groups and communities. For example, a facial recognition algorithm may be accurate overall, but return significantly less accurate results for people with darker skin. Only looking at the overall accuracy score, rather than performance differences across demographics, ignores bias and potential negative impacts on certain communities—often those marginalized because of their race, gender, sexuality, religion, or other protected characteristic. All of an organization's data practices should be examined from disparate impact.

STAGE 2

Analyzing Relevant Legal Frameworks and Ensuring Compliance

Organizations need to understand existing laws in order to maintain legal compliance. Collecting, using, or transferring body-related data may implicate a number of issues under current U.S. privacy law. However, most existing regulations were not drafted with immersive technologies in mind. It can therefore sometimes be unclear how these rules apply in the immersive sector. Further, given that the U.S. privacy law landscape is rapidly evolving, it is prudent to also understand legislative and regulatory trends that may provide insight on what form new regulations may take.

2.1 Understand existing legal obligations

To understand and comply with all existing obligations, organizations need to understand the scope of data types covered by current laws, the requirements and rights that attach to them, and the unique considerations that may apply in immersive spaces and in regard to body-related data.

2.1.1 Data types covered under existing privacy laws

Personal data. Whether U.S. data privacy laws apply in particular circumstances depends on if the information an organization processes is "personal data." Comprehensive data privacy laws often contain a broad definition of personal data, covering data that either is or is reasonably capable of being associated with an identified or identifiable individual.[21] Other privacy laws are limited to specific types of data, such as social security numbers, or data relating to a child. Depending on the data type and law in question, body-related data may be implicated by both categories.[22] Organizations should also be mindful of variations in how laws define subcategories of personal data, such as health data, as this will impact the law's applicability to body-related data.

Biometric data. Under U.S. law, biometric data carries heightened legal requirements. While there is a lack of consensus about what counts as biometric data, several laws govern its collection, use, and disclosure.[23] The issue of what constitutes biometric data has been adjudicated in several cases involving the Illinois Biometric Information Privacy Act (BIPA).[24] However, other U.S. biometric laws exist at the federal, state, and local level, including those that apply in specific contexts, such as education,[25] and these laws often define "biometric data" differently than BIPA.[26] Despite these differences, there are some emerging trends with implications for the use of body-related data:[27]

- Using body-related data to authenticate an individual's identity, such as through face templates or iris scans, is regulated as a biometric.

- Laws with broad definitions of "biometric data" may apply to systems that use face detection, as seen in emerging case law from Illinois regarding virtual try-on XR applications.[28]
- Body-related data not used for identification, such as eye tracking or voice analysis, may be considered biometric if the technology and data are *capable* of identifying an individual, even if not currently used for this purpose.
- Comprehensive data privacy laws often list "biometric data" as a type of sensitive data, which can trigger heightened obligations for processing body-related data.[29]

Biometric laws are particularly relevant for immersive technologies due to the amount of body-related data involved. In an analysis of BIPA lawsuits, the vast majority (78%) of cases alleging consumer harm involved facial scans, with the majority of these cases encompassing virtual try-on services and security and identity verification services.[30]

Sensitive data. State comprehensive data privacy laws designate certain kinds of personal data as "sensitive," and attach additional obligations to their processing. Certain types of body-related data may be included in these definitions, as they can reveal sensitive information about individuals either directly or through additional processing.[31] For example, it is possible to infer ethnicity from hand and head motion data gathered from XR device use,[32] and brain-computer interfaces (BCIs) may provide insight into users' sexual preferences.[33] Though statutes vary in their definition of "sensitive" data, in the U.S. privacy laws are coalescing around a conception that includes, generally: personal data revealing an individual's race or ethnicity, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship/immigration status; genetic or biometric information processed for the purpose of uniquely identifying an individual; personal data collected from a known child; and precise geolocation data.[34] Some laws impose certain duties on organizations related to the processing of sensitive body-related data, such as conducting an impact assessment or obtaining the user's opt-in consent before processing.[35] At the same time, organizations should be mindful of states diverging as to what information is sensitive; body-related data considered sensitive under one law may not be sensitive under another jurisdiction's rules.[36] Outside the U.S., privacy laws have generally adopted an approach to "sensitive" data similar to the EU's GDPR with some country-specific exceptions.[37]

Health data. As with the definition of personal data, privacy laws vary in how they define "health" data. For example, Washington's My Health, My Data Act (MHMD) defines "consumer health data" broadly, including inferences about a person's physical or mental health status that are based on data that is itself not consumer health data. XR, gaming, and other immersive technologies often collect and use a range of body-related data, including eye tracking data,[38] that may reveal if someone has a certain disability or health condition.[39] While the Health Insurance Portability and Accountability Act (HIPAA) only applies to health care providers and related entities, MHMD covers all health information in the consumer context.[40] This means that health data privacy laws like MHMD may apply to body-related data used in immersive technologies when used to deliver fitness, exercise, productivity, or other wellness services. Data used for non-health purposes may also fall within scope if an organization *can* use it to learn more about an individual's health status, although some laws require an organization to actively use it for these purposes to be applicable.

Publicly available data. A number of technologies, immersive and non-immersive, handle body-related data collected in public places. For example, an XR device worn in public may collect data about a user's surrounding environment to optimize graphics, while a vehicle may use sensors to detect the presence of pedestrians.

Some of this body-related data may fall outside the scope of state data privacy laws, such as Virginia's Consumer Data Protection Act (VCDPA), which exempts "publicly available information" from coverage.[41] Many U.S. data privacy laws define publicly available information to include information that a business has a reasonable basis to believe an individual lawfully made available. However, it remains unclear what kinds of information a person can "make available," such as data inferred from public observations. Whether body-related data falls within this exemption could affect stakeholder compliance burdens, an as-yet unresolved question for organizations. Additionally, a lack of clarity from regulators and differences in language across laws has created significant ambiguity for firms to navigate. Organizations should evaluate how and the extent to which to treat this exemption as if it applies to body-related data processing.

2.1.2 Consumer rights under existing privacy laws

Access, deletion, and correction rights. State comprehensive data privacy laws typically grant users the rights of data access, deletion, and correction, and require that these rights may be exercised in a manner that is consistent with how a person would normally interact with the entity.[42] Organizations should make intentional decisions about how to provide for the exercise of these rights considering the unique ways users may interact with immersive technologies. Organizations should also understand how any differences between laws affect their compliance obligations with regard to offering these rights. For example, the Delaware Personal Data Privacy Act (DPDPA) is unique among comprehensive privacy laws in the U.S. in granting individuals an affirmative right to "obtain a list of the categories of third parties to whom the controller has disclosed the consumer's personal data."[43] Since immersive technologies may transmit body-related data to third parties for certain uses such as multi-user experiences, these requirements may impact organizations' obligations.

Consent: opt-in, opt-out, manipulation, and so-called "dark patterns." Data privacy laws often require organizations to obtain consent before processing personal data, though laws may differ in their triggers for consent and vary in the type of consent required in particular circumstances.[44] Some data privacy laws also prohibit the use of "manipulative design" that may pressure users into providing consent, as the person's consent would be considered to be neither "informed" nor "freely given."[45]

2.1.3 Business obligations under existing privacy laws

Transparency and notice. Among other things, transparency provisions in U.S. privacy law require organizations to provide information to individuals about their processing of personal data. Providing notice regarding body-related data in immersive environments may be challenging, given their three-dimensional nature, the variety of body-related data they use, and the potential capture of bystander data.[46]

Data minimization. Data minimization provisions in U.S. privacy laws commonly require organizations to limit the processing of personal data to that which is needed for a specified purpose. Laws may also require organizations develop data retention schedules for deleting data after a given period of time.

DPIAs. U.S. data privacy laws may require organizations to conduct impact assessments or similar documentation when processing body-related data.[47] Given that processing body-related data can potentially result in harmful outcomes,[48] it may trigger DPIA requirements, and organizations should evaluate how these laws define "harm."[49]

Protections for kids and teens. The Children's Online Privacy Protection Act (COPPA) confers special protections to the data of children under 13, and some state data privacy laws contain heightened protections for teens.[50] Nearly all body-related data that immersive technologies collect about children will likely be regulated as "personal information" under COPPA.[51] However, some data may fall outside of this definition, particularly when it is processed on device,[52] and the precise contours of how COPPA will apply to immersive technology data remains uncertain.[53]

Unfair and deceptive practices. Under the Federal Trade Commission (FTC) Act and state statutes, any time that an organization's disclosures do not match their data practices the organization could be found to be engaging in deceptive acts or practices.[54]

2.2 Understand the changing legal landscape

New legislation and regulations will continue to impact the data privacy legal landscape. In the U.S., states have led the way in enacting data privacy laws in the absence of comprehensive federal rules. Major areas for emerging legislation in 2023, for instance, included youth privacy and safety,[55] as well as consumer health data.[56] Organizations should also monitor how emerging litigation impacts current requirements through interpreting current legislative language.[57]

STAGE 3

Identifying and Assessing Risks to Individuals, Communities, and Society

In addition to legal compliance, leading organizations also seek to mitigate risk by ensuring their products, services, and other uses of body-related data are fair, ethical, and responsible.[58] They proactively identify and minimize the risks their data practices could pose to individuals, communities, and society. While it can be difficult to operationalize high-level principles like "fairness"—particularly for emerging technologies like XR—there are a number of considerations that organizations can make when developing their data practices. Data practices that embody these principles can signal to the public what the organization's values are, and help earn user's trust that they are handling their data in accordance with users' best interests.

As demonstrated in the chart on the following page, privacy harms may stem from particular types of data being used or handled in particular ways, or transferred to particular parties.[59] Privacy laws in the U.S. often focus on data type, by regulating categories like "sensitive data," rather than data use.[60] While it could be—and has been—argued that it is actually the *use* of data or context in which a given data practice occurs that is more directly relevant to the privacy risk,[61] even the collection of data in the first place raises the risk of a potential harm to the data subject.

Body-related data, and particularly the aggregation of this data, can give those with access to it significant insight into an individual's personal life and thoughts. This includes not just an individual's unique ID, but potentially their emotions, characteristics, behaviors, desires, and more.[62] Because immersive technologies are evolving rapidly, it is not always possible to know exactly what insights or inferences any given piece of data may be able to provide in the future as data analysis techniques improve.[63] As such, data that is generally "low risk" or not considered "sensitive" may, at some point, be capable of revealing "high risk" or "sensitive" information.[64] Additionally, if data ends up being transferred to another party, it is not always clear how *they* may use it in the future.

3.1 Identify risks related to data type

3.1.1 Identifiability

Body-related data that is identifiable is typically considered "biometric data."[65] Biometric data is particularly sensitive because it is inherently tied to each individual, and could be used to facilitate identity theft, security breaches, and personal profiling. Different types of body-related data vary in their identifiability, and it is important to remember that identifiability is not static. For example, fingerprints currently have high identifiability, and the ability to identify individuals by their face has been increasing in recent years.[66] However, there was a time when the capability to identify people with these data types did not exist. Likewise, in the future it is likely that other body-related data types such as gait and hand movement will increase in identifiability.[67] Organizations should consider how likely it is that each type of data could be used to identify

STAGE 3

FACTORS RELATED TO RISK	FEATURE	CONSIDERATIONS
Data type	Identifiability	Ability to uniquely identify someone; ability to link other data to a uniquely identified person; ability to infer unique identity
	Sensitivity	Characteristics covered by law (race/ethnicity, religious beliefs, mental or physical health condition or diagnosis, sexual orientation or behavior, citizenship or immigration status, consumer health data, genetic or biometric data, data of a known child, status as a victim of crime, precise geolocation, etc.); ability to infer sensitive data categories from non-sensitive information; targeting and personalization based on sensitive data categories
	Potential for inferences	Ability to identify or infer information about an individual, including their internal state
	Data accuracy and bias	How accurate and/or representative data is; existence of bias
Data handling	Critical decisions	Whether a data practice is impacting an individual's access to housing, credit, insurance, the legal system, healthcare, education, career opportunities, or public benefits
	Partners and third parties	How likely a partner or third party is to collect, use, and onwardly transfer data lawfully and fairly
	Data retention	Length of time data is kept, particularly in identifiable form
	User expectations and understanding	User familiarity with data types and uses; how aware users are of data collection or use; level of detailed understanding of data practices

someone now or in the near future, and institute protections accordingly.[68]

In evaluating identifiability, organizations should consider the following attributes:[69]

- **Direct identifiers** can be used to identify an individual by itself, with no additional data (e.g., facial recognition).
- **Indirect identifiers (pseudonymized data)** can be used to identify an individual only with the addition of other data (e.g., data about a user's gameplay in an immersive experience, which could be tied to a profile).
  - *Linkability to other datasets*: The ability to identify an individual using indirect identifiers increases with the ability to link different sources of data together, particularly when direct identifiers are included as a data source. An individual's identity may also be inferred based on their behavior.

- **De-identified/anonymized/aggregated data** cannot be reasonably linked to an individual's identity, profile, or device (e.g., aggregate data of all users' body movements within a game).

3.1.2 Sensitivity

Certain types of data may be considered "sensitive" if they could more easily lead to harms like discrimination, embarrassment, or reputational damage.[70] In recognition of this, a number of privacy regulations place enhanced protections on "sensitive" data.[71] Immersive technologies may collect data that is considered sensitive—either by statute or by cultural norms—such as geolocation or information about a person's neural activity. Even if data is not sensitive on its face, with the increasing ability to make inferences about individuals based on pieces of personal data,[72] the line between "sensitive" and "non-sensitive" data is blurring.[73] For example, it is possible to infer, with relatively high accuracy, "sensitive" data categories such as the sexual orientation and health condition of VR users based on "non-sensitive" data like eye and body movement.[74] In some jurisdictions, the use of legally "non-sensitive" data to make "sensitive" data inferences constitutes the collection or use of "sensitive" data, and the relevant protections should apply.[75] But as technologies improve, it is less clear when certain types of data—such as eye or body movement—should be considered inherently "sensitive" data.[76]

Immersive technologies hold the potential to be widely used across sectors,[77] and certain sectors are subject to privacy laws because of their more sensitive nature. For example, healthcare and patient data is covered by HIPAA,[78] and student data is covered by the Family Educational Rights and Privacy Act (FERPA).[79] Organizations dealing with data in these specific contexts incur higher legal risk, and should also be mindful of how sectoral regulations signal the sensitivity of certain data practices. They should also recognize that context is key to privacy, and that disclosing data carries different risks and considerations across contexts and sectors.[80]

3.1.3 Potential for inferences

Data that can be used to make further inferences about people carries additional risks. While some of these inferences may qualify as "sensitive data," others may not. Increased data collection, paired with ML and other data processing techniques, has led to an increase in "probabilistic predictions," or inferences. Whether accurate or not, inferences about people's identity or sensitive characteristics can be invasive, creating a profile of an individual with information they may not have consented to share.[81] Because inferences can be made from seemingly unrelated data, individuals are often unaware what data informed the decision—or that the inference was made in the first place. Additionally, particularly in high-risk or critical contexts like law enforcement, decisions made based on inferences can be dehumanizing and harmful, denying dignity to those subject to the profiling.[82] The amount of data and processing capabilities present in immersive environments means it is possible to more accurately infer sensitive characteristics—such as age, gender, and certain health conditions—from body-related data collection.[83]

Immersive technologies also allow for what is called "*biometric psychography,*" which has been used to describe "behavioral and anatomical information used to identify or measure a person's reaction to stimuli over time, which provides insight into a person's physical, mental, and emotional state, as well as their interests."[84] Immersive technologies allow data collectors to access not only data that is *emitted* from a user's body, but also the external stimulus to which the user is *reacting*, granting further insight into their internal state. The range of sensors and processing techniques integrated into immersive technologies means that data like eye tracking, pupil responses, facial scans, and more could be combined and aggregated to infer information that users did not intend,[85] including health conditions, cognitive processes, and likes and dislikes—potentially for the purpose of manipulation.[86]

3.1.4 Data accuracy and bias

If an organization does not proactively monitor its data practices to ensure they are accurate and unbiased, it may result not only in harm to users, but also in a poorly functioning product or feature. A major source of inaccuracy and bias in technologies is the source from which organizations collect or receive data. Applications that are not trained on broad and diverse sets of data are likely to vary in performance across demographic groups, reflecting the makeup of the initial training data and leading to biased outcomes.[87] In the context of immersive technologies, some potential examples of bias arising from unrepresentative data and algorithms could include:

- An application that diagnoses health conditions like Parkinson's disease based on body movements in VR could under-diagnose certain segments of the population, leading to worse health outcomes.
- A neurotechnology program that provides productivity recommendations based on neural activity could be less effective on certain users, leading to performance disparities.
- A tool that infers a user's interest in a given advertisement or piece of media based on gaze and level of interaction could misinterpret certain users' behavior, leading to less helpful personalization.

Looking at the aforementioned examples, there could be serious consequences for individuals if there is inaccuracy or bias in an application that makes inferences or decisions about their health, performance levels, or attention, including discriminatory outcomes based on race, gender, sexual orientation, or other protected traits. These outcomes can translate into legal repercussions for organizations. In 2023, the FTC indicated the agency's intent to crack down on "unfair and deceptive" practices involving inaccurate and biased data in the context of automated decision-making systems.[88]

Accuracy in Emerging Body-Related Data Types

Certain data types and uses may be less reliable, particularly if they are new or not robustly tested. Accuracy can be an issue both for identifying an individual or for making inferences about their characteristics or behavior.[89] For example, a system built to analyze only an individual's gait and make inferences about their health status may likely be less accurate than other, more holistic diagnostic methods.[90] That said, with more research these systems may, and often do, become more accurate.

To the extent possible, organizations that handle body-related data should ask themselves:

- **Is the data representative of the organization's target community at large?** Algorithms will be biased if they are trained on data that excludes or over-indexes certain demographic groups, based on race, gender, age, disability status, language, and many more characteristics.
- **If there is inaccuracy or bias, what is the source?** Inaccuracy or bias could arise out of the organization's own practices, or from data collected from another source. Data may be biased if it is incomplete or unrepresentative, or if it is drawn from historical data reflecting societal inequities. Bias may also come from how an algorithm is designed, based on which factors a human developer chooses to include and how to weigh them.[91]
- **Is targeting or personalization leading to discriminatory outcomes?** Creating a personalized experience for users can lead to discrimination if certain communities are overall more likely to be excluded from seeing critical life opportunities, such as housing rental options. Such exclusion may trigger legal liability under civil rights laws.[92]

- **Who is best placed to identify issues with the data, and what mechanisms can be put in place to spot and correct these issues?** Organizations can include those with expertise in identifying bias and its underlying causes in multidisciplinary teams made up of staff from product, policy, legal, engineering, data science, and government and public affairs, who can work together to flag any risks.[93]
- **Is data collected, used, or disclosed for the purpose of ensuring anti-discrimination commitments or goals?** Some organizations adopt practices to combat existing bias or inequity, which may require them to collect additional demographic data which itself may be sensitive. There may thus be a tension between an organization's equity efforts and commitment to data minimization. Weighing these goals is a complicated process that will often be unique to any given organization, but at the very least organizations should be as transparent as possible about their practices and intentions.[94]

3.2 Identify risks related to data handling

3.2.1 Critical decisions

When personal information—or inferences based on this information—is used to inform critical decisions about people's lives, there may be a greater risk of potential harm, particularly without adequate notice, consent, and an opportunity to opt out. Automated decision-making tools can be used to make decisions related to housing, credit, insurance, the legal system, healthcare, education, career opportunities, and public benefits.[95] When there are problems with these systems—either in the training data, algorithm, or implementation—there is a high risk that they will have discriminatory outcomes.[96]

Heightened risks may also occur in advertising, such as if certain demographic groups are excluded from seeing content related to careers, education, and other opportunities.[97] The breadth and depth of data in immersive spaces allows for even more granular targeting, personalization, and profiling, potentially on the basis of a sensitive data category.[98]

AI and Immersive Technologies

As AI is increasingly integrated into immersive technologies, it is likely to make virtual spaces more immersive, appealing, and accessible by allowing users to more easily create their own visual, audio, and text content.[99] At the same time, more integration between AI and immersive tools raises risks related to privacy and safety.[100] For example, bad actors could exploit the wealth of intimate data generated in immersive environments to create even more manipulative influence campaigns.[101] As such, organizations that use AI within or alongside immersive technologies should evaluate additional potential risks when deciding if and how to offer such features, particularly when involved in making critical decisions.[102]

3.2.2 Partners and third parties

Immersive technologies are often part of a data ecosystem, in which different entities collect, process, and further distribute data amongst one another. For example, a VR headset might collect a user's eye data, and transmit this data through APIs with third-party developers who create applications for the headset.[103] Organizations should understand their position in this ecosystem, in terms of both who is sending them data and to whom they are sending it.

Some questions to ask when receiving data from another entity include:

- Have you verified or otherwise ensured that the entity from whom you are receiving data took appropriate steps to collect any data legally and ethically?
- Could the data contain inaccuracies or reflect any bias?
- Was the data collected in a particular context, or for a particular use, and is there a process to remove or delete that data after it is no longer needed or appropriate?

- Does the data include data subjects who are known children,[104] or who fall within any other population who might be subject to specific regulations?[105]

Some questions to ask when transferring data you have collected to another entity include:

- Have you verified or otherwise ensured that the entity to whom you are sending data will handle it in a responsible manner, and to follow any relevant policies or terms of service?
- Do certain entities to whom you are transferring data create particular risks, either in regard to their industry, known plans for the data, or some other factor? Does transferring data to such entities have the potential to cause harm or have a disparate impact on certain individuals or communities?[106]
- What mechanisms do you have for monitoring third-party actors' downstream data practices, and how do you enforce compliance with laws, contracts, and policies in this regard?
- If offering a product or service that includes a software development kit (SDK) developed by a third party, how are you ensuring the third-party SDK provider is engaging in safe, privacy-protective practices?[107]

3.2.3 Data retention

Keeping data longer than is needed to perform specific, identified functions raises a risk that data will be used in a way that harms individuals or communities, particularly if kept in identifiable form.[108] Additionally, the longer data is kept, the less accurate and useful it will often be, degrading the models that it is used to train.[109] While many immersive technologies require personal data, they do not always require that data be retained beyond brief periods around the time of collection. Whether and for how long an organization retains body-related data will depend on the specific purpose for which it is used; some common purposes include mapping a user's immediate surroundings, creating a profile of a user, and fulfilling statutory data retention requirements.[110] While certain uses may require organizations to keep data for extended periods of time, this does not mean organizations should retain it indefinitely.

3.2.4 User expectations and understanding

The details of an organization's immersive technology data practices may surprise people who do not receive full disclosure of those practices,[111] either in regard to novel types of data, such as data on gaze, or novel uses of data, such as for inferring a person's emotions.[112] Studies have shown that people value when organizations are transparent about their data practices,[113] and lose trust when their practices do not align with their promises.[114] Determining people's expectations of privacy is complicated, particularly because it may vary between individuals and populations. Gaining insight into what expectations relevant people have about your organization or product often requires early and ongoing engagement with users and potential users. Engagement must extend beyond the initial point of data collection or use and also include how data is repurposed or used later on.

Individuals may feel more surprised by data practices that are further distanced from the point of data collection, or where the benefits are not directly understood. Sources of data collection for immersive technologies include data that is:[115]

- Collected **directly** from individuals (e.g., profiles that users fill out themselves)
- Collected **indirectly** (e.g., face detection or analysis of a bystander in the vicinity of an XR device)
- **Gathered** or **derived** by an organization (e.g., time spent in an application), including data collected from users' **unconscious** or **involuntary** behavior (e.g., gaze data)
- **Inferred** from other data (e.g., user interests inferred from gaze and body movement data)
- **Purchased** or **obtained** from another party (e.g., a third-party application receiving user data from a first-party platform through an application programming interface, or API)

Additionally, the interfaces common in immersive technologies—such as XR headsets or wearable

devices—sometimes differ significantly from traditional online spaces. Providing notice of the organization's data practices may therefore need to look physically different than traditional disclosures or standard privacy policies.[116] The system of disclosures that has been built around current technologies is geared toward web and mobile applications, and not necessarily for novel immersive interfaces.[117] For example, a pop-up check box might not be as effective in a VR environment as on a desktop website (to the extent the latter is itself effective at educating users).[118]

Another challenge to ensuring proper individual understanding of an organization's data practices is for organizations to determine how to avoid overwhelming individuals with information. Due to the scale of data collection in immersive environments, the various data uses, and potential disclosure arrangements, it is difficult to provide notice to users about data practices in a way that is comprehensive yet understandable.[119] Determining proper notice becomes even trickier when communicating in ways that are appropriate for audiences of different ages and cognitive ability. That said, while notices and disclosures are an important part of protecting user privacy, and for educating users about new data types and uses, they are just one tool among many for protecting privacy.[120]

3.3 Assess fairness, ethics, and responsibility

Once an organization understands its data practices, legal obligations, and the risks associated with the use of body-related data in immersive environments, the organization must assess whether and to what extent their practices actually implicate any of the potential risks. In the absence of broad consensus on what practices are considered fair, ethical, and responsible in the context of immersive technologies,[121] organizations can ask:

- Does a data practice raise a specific risk to individuals, communities, or society?
- What are the harms that each risk may create, and how severe might they be?
- Who is likely to be the most significantly harmed by the realization of any given risk?
- Taken as a whole, do an organization's data practices as a whole raise risks to individuals, communities, or society? For example, does the collection of hand movement data, unique identifiers, and other categories of data raise risks that are not raised by any single data category in isolation?
- Might technology change in the near future in a way that makes certain data practices more or less likely to result in harm, or more or less harmful?

Organizations can also ask if there are particular elements of their data practice that raise the severity or likelihood of a harm occurring, including:

- Is collected data able to uniquely identify someone, or is it linked with other data that could uniquely identify them?
- Does collected data belong to a "sensitive data category," such as health condition or sexual orientation, or does it allow the organization to infer a sensitive data category?
- Can collected data be used to identify or infer an individual's mental or emotional reaction to content or stimuli?
- How directly is data collected from individuals, and how aware are they of this collection?
- Is data being used to inform or make consequential decisions for individuals, such as whether a certain person gets access to housing opportunities or healthcare?
- How closely does a particular use of data resemble the use for which the data was originally collected?
- Is a partner collecting, using, and/or further transferring data in a fair and lawful manner?
- Is collected data regulated by sectoral laws?

There is no "right" approach to evaluating an organization's data practices in regard to fairness, ethics, and responsibility. However, in thinking about how their data practices align with their organizational objectives, it is helpful to ask:

STAGE 3

- What organizational goal or objective is a given data practice serving?
- Is there a rational link between a particular organizational objective, such as providing a feature or service, and the data practice? For example, if the purpose of collecting eye tracking data is to enable eye-based controls, then it would be far removed to use that data to make inferences about user interest for the purpose of serving targeted advertising.
- Is a given data practice *proportionate* to a particular organizational objective, or for providing a feature or service in a way that weighs the privacy risks with other organizational equities? For example, if eye tracking for the purpose of enabling eye-based controls requires a first party to transfer this data to another party, the first party should only transfer this data with the required party for the specified purpose.
- What value or benefit are users getting from an organization's data practices?
- Which, if any, public policy or legal considerations will impact the organization's analysis of whether its data practices are fair, ethical, and responsible? For example, organizations may need to collect additional data about children for the purpose of complying with legal requirements around age verification.
- Are there any alternatives to a given data practice that are more privacy-friendly, while still allowing the organization to achieve its objectives?
- Does a given data practice raise risks that are too significant or implicate sufficiently serious harms such that it should be abandoned altogether?

LOWER RISK	HIGHER RISK
Involves limited personal data	Involves a large amount of personal data or data processing on a large scale
Does not involve the personal data of vulnerable or marginalized populations	Involves the personal data of one or more vulnerable or marginalized populations
Does not involve location data or sensitive personal data (including "biometric psychography")	Involves location data or sensitive personal data (including "biometric psychography")
The context is not sensitive	The context is sensitive
Has a minimal impact on individuals or communities	Has a major impact on individuals or communities
Involves one-time or short-term data collection and use	Involves ongoing or longer-term data collection or use
Does not involve profiling, evaluation or scoring of individuals	Involves profiling, evaluation, or scoring of individuals
Does not involve automated decision-making with legal or similar significant effect	Involves automated decision-making with legal or similar significant effect
Does not involve the collection of data in public places	Involves the collection of data in public places
Does not involve an unfamiliar data type or use	Involves an unfamiliar data type or use

Adapted from FPF's Mobility Data Sharing Assessment.[122]

STAGE 4

Implementing Relevant Best Practices

There are a number of legal, technical, and policy safeguards that can help organizations maintain statutory and regulatory compliance, minimize privacy risks, and ensure that immersive technologies are used fairly, ethically, and responsibly. These best practices should be implemented in a way that is **intentional**—adopted as appropriate given an organization's data practices and associated risks; **comprehensive**—touching all parts of the data lifecycle and addressing all relevant risks; and **collaborative**—developed in consultation with multidisciplinary teams within an organization including stakeholders from legal, product, engineering, privacy, and trust and safety.

Importance of Multidisciplinary Teams

Decisions about data practices should be made in consultation with a range of stakeholders from across the organization, who each bring a unique and valuable perspective. Consultations should be done at various decision-points: creating and implementing privacy programs, operationalizing high-level organizational goals, spotting issues with data, balancing privacy with other equities, and engaging in DPIAs and other similar audits. An example of what a multidisciplinary team could look like includes:

- **Government affairs:** understands the regulatory environment, can consult on general best practices
- **Legal:** ensures compliance
- **Product:** knows user expectations and the direction design is going, can help design better data flows
- **Engineering:** knows what is technically feasible, can implement PETs
- **Privacy:** understands privacy risks and organizational data flows
- **Trust and safety:** knows user concerns, best practices

The following best practices for organizations are drawn from well-established principles and protocols, customized to address the unique challenges related to body-related data in immersive environments. These practices complement and strengthen one another, and should be considered collectively.

4.1 Implement best practices

4.1.1 Data minimization

RECOMMENDATIONS

- Implement technical tools such as privacy-enhancing technologies (PETs) and design approaches like privacy by design to put data minimization into practice.
- Limit exploring new body-related data types and uses to lab and pre-deployment settings, rather than with live user data.
- Develop internal data retention policies based on how long data must be kept in order to achieve a stated objective or provide a stated service.
- De-identify or dispose of data once it is no longer needed.

STAGE 4

Data minimization involves limiting data processing to that which is necessary to fulfill specific objectives or provide specific features.[123] Operationalizing data minimization can be difficult for products like immersive technologies that rely on large amounts of data: even if data collection is limited to only what is needed to provide a feature, it still may involve significant amounts of personal data.[124] That said, data minimization is an important first step for building a robust privacy program.

In operationalizing data minimization as a practice, organizations should consider how to implement both technical tools such as privacy-enhancing technologies (PETs) as well as design approaches like privacy by design. Even when data must be collected in order for a technology to function, these strategies may help minimize privacy risks.[125] For example, PETs, such as differential privacy, could allow organizations to collect necessary data while also maintaining individual privacy and anonymity.[126]

DATA MINIMIZATION APPLIED: EYE TRACKING

In the context of immersive technologies, organizations that wish to collect eye tracking data should limit the collection of eye data to only what is necessary to serve a particular stated purpose. For example, using eye tracking to power more expressive avatars will require gaze data, but not necessarily pupillometry data.[127] Other uses, such as measuring visual fatigue or determining user interest in particular content, will require more data, which may pose higher risks.[128] Organizations should evaluate whether the risks are too high to carry out safely, and if they decide to move forward with these uses, should institute further safeguards—such as strong user controls and retention limitations—to minimize these risks. When possible, organizations should also refrain from collecting data about what content a user looks at and for how long.

If organizations want to explore new uses of body-related data, they should consider limiting this to pre-deployment settings, rather than with live user data. Specifically in regard to new products and use cases, there may be an incentive to collect as much user data as possible upfront and figure out how to use it later.[129] Organizations should refrain from using live user data to try out new features; instead, they should conduct rigorous testing and assessment before release to ensure any novel use is safe. Pre-deployment testing should be done in controlled environments with proper controls in place, and in conditions that will resemble real-world use as closely as possible to prevent bias, inaccuracy, or discrimination in the product once it's released. In some instances, organizations may have the opportunity to explore developing these technologies in regulatory sandboxes, which allows for experimenting under the supervision of a regulatory authority.[130]

Limiting the amount of data organizations retain can also help lower the risk it will be misused. Organizations should develop internal data retention policies based on how long data must be kept in order to achieve a stated objective or provide a stated service, and de-identify or dispose of data once it is no longer needed. Data should not be kept indefinitely, especially in identifiable form. Particularly for high-risk data types, data should only be stored for as long as is necessary to provide a particular function that the organization has articulated. If high-risk data needs to be stored over time, additional safeguards should be implemented as appropriate. Safeguards might include on-device storage, encryption, and allowing users to have more granular control over how the data is used. In some cases, organizations may have to retain data for an extended period of time for legal reasons, such as to conduct an audit or risk assessment. Novel data types in particular should

have short retention periods. Most people are likely to consider that data about where they are looking or the dilation of their pupils is especially sensitive. If this data is no longer needed, it should be deleted right away—it should only be retained if there is a specific purpose for it.[131]

RETENTION LIMITATIONS APPLIED: EYE TRACKING

Because eye tracking data could potentially reveal sensitive information about an individual's preferences and characteristics, an organization collecting it may decide to retain only information about what a user ultimately "clicks" on, rather than all of the content they have looked at.

4.1.2 Purpose specification and limitation

RECOMMENDATIONS

- Be as specific as possible when identifying data processing purposes.
- Avoid collecting, using, or transferring data beyond the original stated purposes without additional action.

Closely related to data minimization is the practice of purpose specification and limitation: clearly and accurately communicating the purpose of any given data processing activity to users prior to processing, and not going beyond these stated purposes.[132] This process goes hand in hand with data minimization, as an organization's purpose for engaging in a data practice will determine what data is needed in the first place, and thus how to minimize data collection.

The purposes for data processing that organizations identify should be as specific as possible. Organizations should avoid overly-broad justifications like "product improvement," which do not communicate enough information to users about a data practice's purpose and leave the door open to broad and expansive future uses. Specificity also helps to limit the potential that overly risky processing will occur.[133]

If organizations want to collect, use, or transfer data beyond the original stated purpose, they should engage in additional action.[134] When these practices result in quantifiable harm, the FTC may consider them "unfair" or "deceptive" practices, subject to enforcement action.[135] However, even when these practices do not result in quantifiable harm, users may feel violated. Organizations that wish to expand their data processing beyond initial use should take additional steps prior to doing so.[136]

PURPOSE SPECIFICATION APPLIED: EYE TRACKING

For lower-risk data practices, notice by itself may be sufficient: for example, an organization that wants to expand its use of eye tracking only to provide more expressive avatars, better balance and anti-nausea mechanisms, and eye-based controls, could provide clear and conspicuous disclosures of these data uses. However, for higher-risk data practices—such as using eye tracking to measure a user's interest in content—consent should also be obtained.

4.1.3 Transparency: meaningful notice and consent

RECOMMENDATIONS

- Provide notice and obtain consent in context, without overwhelming users.
- Use immersive technologies' unique interface to provide users with more intuitive, effective product and data practice education.
- Ensure that when users give consent, it is specific, informed, and freely given.
- Start users with the most privacy-protective default settings and allow them to alter their preferences.

Most organizations understand that they need to be open and honest with both users and the general public about their data practices, but it is not always clear exactly how this should look in practice. Education is key for building trust, and organizations that handle body-related data in immersive environments may need to be even more proactive about informing users of their data practices.

As such, organizations must provide notice and obtain consent in context, without overwhelming users. Organizations need to consider *transparency*—providing adequately granular information about and controls over data practices—as well as *usability* and *effectiveness*—not overwhelming the user, which could lead to consent fatigue or degrade user experience. While this may be difficult to achieve, design techniques like "progressive disclosure" can gradually ensure that users are familiar with the organization's data practices without bogging down the experience with notices.[137]

Because of immersive technologies' unique interface, it may be possible to design novel methods of providing notice and obtaining consent that are more natural and effective.[138] For example, in XR environments, instead of the pop-up box found in traditional online spaces, which may "break" the immersive effect, an avatar or non-playable character could explain data practices to users. Organizations can also design notices such as "ambient notifications" that fit organically into the context and interface of an application without interrupting users' experiences.[139] Because immersive environments often contain multiple data modalities, organizations should investigate how to design more accessible notice and consent practices, taking advantage of the unique design capabilities available and accommodating users based on considerations like disability or culture. Human-computer interaction designers should continue exploring these possibilities.[140]

When designing products, organizations must ensure that user consent is specific, informed, and freely given. An organization's legal team should be able to provide guidance on compliance with privacy laws' notice and consent requirements as needed. When handling children's data, organizations should also follow legal guidelines and best practices for obtaining verifiable parental consent and avoid using manipulative design practices to coerce users into providing consent.[141] Notice and consent should occur within the context of an experience or application; merely linking out to a privacy policy on a website is not sufficient.[142] The consent options given to users should also not be binary: users should have the ability to select settings that more closely reflect their preferences from a menu of options. In multi-player applications, this will require designing the experience in a way that allows users with different preferences to interact with one another.[143]

Default settings can go a long way towards protecting user privacy. In order to fully respect an individual's privacy preferences, organizations should start with the most privacy-protective settings and allow users to alter them later on. In the context of VR, for example, organizations should automatically start users off with virtual safety boundaries around their avatars and the ability to block other users.[144]

TRANSPARENCY APPLIED: EYE TRACKING

In order to provide users with a deeper understanding of how eye tracking works, organizations can design "visceral" notices that provide a more intuitive, experiential understanding of their data practices. In other contexts, "visceral notice" includes things like rumble strips on roads and blinking lights on video conferencing applications.[145] In the context of VR and eye tracking, visceral notice could include on-screen icons that indicate when eye tracking is on and where users are looking, or consent mechanisms that require users to look at different virtual objects, demonstrating how eye tracking works.[146] Default settings also help ensure that data processing does not occur without informed consent. For example, features like eye tracking could be off by default, and users are able to turn them on if they wish to do so after being notified about how it works and how the data is used.

Organizations can implement a combination of notice types that provide sufficiently granular information to users about their data practices without inducing consent fatigue or sacrificing the immersiveness of the experience. These notice types include:

NOTICE TYPE	DESCRIPTION
Layered notice	Provides a condensed notice with key information up front and the option to expand the notice to learn more[147]
Contextual notice	Highlights data practices that might be unexpected given the context[148]
Just-in-time notice	Appears when a user wants to access a relevant feature, rather than at sign-up or at the first point of access[149]
Data dashboard	Allows users to manage data preferences all in one place with an interactive "menu" interface[150]
Visual notice	Explains privacy and data practices with a "nutrition label"[151]
Visceral notice	Uses design techniques to provide users an "experientially resonant means of understanding privacy threats"[152]

BYSTANDER PRIVACY

XR devices, and any technology that engages in public data collection, may incidentally collect data about bystanders.[153] Providing privacy notices to bystanders, and obtaining their consent, is incredibly difficult to do effectively, making notice and consent alone inadequate for protecting bystander privacy. While it is possible (and recommended) to implement "notice" features like lights that signal to bystanders when an XR device is recording,[154] such practices will not rise to the level of adequacy needed for legal notice. Organizations should also engage in data minimization, and implement relevant PETs when appropriate,[155] such as automatically blurring the faces of bystanders.[156]

4.1.4 User controls

RECOMMENDATION

- Allow users to access, correct, and delete their data.

Users should be able to access personal data collected about them, correct it when inaccurate, and delete it when possible.[157] Organizations should provide users with the ability to exercise these functions in a clear, conspicuous, and contextual way. It should be designed so that it is intuitive and accessible for the given medium, based on how users act in immersive environments.[158] Users should also have the ability to tailor their experience to their privacy preferences to the extent possible without having to conform to strictly binary decisions. For example, if users wish to delete data organizations collect about the content they look at, they should be able to do so.

4.1.5 Local and on-device processing and storage

RECOMMENDATION

- Process and store as much data on a user's device as possible.

Organization's should process and store as much data on a user's device as possible, which may lower the chance it will be misused.[159] It is particularly important that higher-risk data—including data that is identifiable or belongs to a sensitive data category—be processed and stored in encrypted form as close to the data source as possible. For example, organizations can process and store eye tracking data about what users look at on their device, rather than send it to a server or third party.[160] There are some limitations to this approach. Many of the emerging capabilities in immersive technologies require significant computing power, which personal devices may not have. It is also more difficult to update any necessary algorithms when data is processed or stored on-device, rather than remotely, potentially leading to worse functionality or security vulnerabilities.[161] That said, to the extent possible, and particularly for higher-risk data types and uses, on-device processing and storage should be considered as part of an organization's privacy program.

4.1.6 Third party management

RECOMMENDATIONS

- Conduct due diligence to ensure potential third-party data partners abide by compatible privacy policies.
- Develop and enforce policies by which third parties must comply in order to maintain partnership.
- Create internal policies regarding transmitting data for research and government requests for data.
- Limit transmitting data to only what is needed to achieve an objective or provide a service.
- Explore other technical and organizational tools for third party management.

The immersive technology ecosystem is made up of a web of organizations that disclose data to one another, each one providing different functions and experiences.[162] For example, an entity that makes an XR headset might transfer data to an entity that operates a platform, which might transfer data with third-party app developers. But disclosing data to others can open up the possibility that the third party will use the data in an unexpected or harmful way that does not align with an organization's interests or those of its users.

Before partnering with another entity to transfer data, organizations should conduct due diligence to ensure their potential partner abides by compatible privacy policies, to minimize the risk

of downstream data misuse.[163] Organizations can also conduct data flow analyses on potential third parties to ensure that an application's data flows match their privacy policies.[164]

After vetting potential data partners, organizations should develop policies by which third parties must comply, and implement contractual restrictions on any data that is disclosed. By building privacy protections into contracts, organizations can minimize the risk that data they transfer will be misused by other actors. Such contractual restrictions could require third parties to:

- Develop and implement appropriate privacy and security policies and practices.[165]
- Use data only for specific, disclosed purposes.
- Get access to only the data that is necessary for providing a particular product or service.
- Set terms for how long the third party is allowed to retain or use data, and how they will treat the data once they are no longer using it for providing a product or service.
- Refrain from re-identifying data.
- Ensure that any other downstream parties or subcontractors also adhere to contractual restrictions.[166]

Organizations should have dedicated team members with the bandwidth to perform ongoing monitoring for third party compliance with contractual obligations—for both their stated privacy policies as well as their actual practices. There should also be processes in place for remedial action in the event of a third party's breach of contract, or if the third party's practices violate any other legal obligations.

Personal data should only be transferred to third parties in situations in which it is needed to achieve an objective or provide a service. The context in which data is collected is important: personal information collected in one context may not be appropriate when used in another context.[167] As such, when data must be transferred to entities beyond which an individual has already been made aware, the collecting organization should get additional informed consent to do so, and the data should be limited to that which is relevant to provide their stated product or service.

Organizations should also ensure that they have appropriate internal policies regarding non-commercial requests for personal data. For example, organizations should have policies around when and how to partner with academics, allowing them controlled and privacy-protective access to personal data in order to study and improve education, public health, and societal knowledge and progress in other scientific areas.[168] On the other hand, organizations should ensure that data requests from government actors like law enforcement satisfy constitutional standards of due process and other statutory requirements. Organizations should create guidelines on when and how staff should comply with such requests, and publicly disclose what requests they received and whether they complied.

TRANSFER LIMITATIONS APPLIED: EYE TRACKING

Even within a single category of data, there can be nuance around what data to which a third party is granted access. For instance, not all uses of eye tracking data require every piece of information about an individual's eye. Organizations may limit the data they disclose only to the relevant "events"—eye movements, fixations, and other such functions—that are necessary.[169] Limiting data transfers lowers the risk that a third party will use data in a way that surprises or harms a user.[170]

While the best way to minimize risk is to not transfer data to third parties when they do not need it, first parties can also implement other administrative and technical measures, and audit and enforce compliance with contracts. Such measures could include:

- Aggregate data, apply noise to data (differential privacy), or create synthetic data to reduce the ability for third parties to profile users.
- Develop app store-style permission systems, which require third-party applications to be "certified" to run on their platform.
- Deploy trusted execution environments (TEEs), which create isolated environments within main processors that allow multiple parties to access data while also protecting it from unauthorized access, while the data is in use.[171]
- In order to minimize the risk of data overcollection or misuse when contracting with SDK providers, establish SDK governance policies, conduct due diligence before entering into contracts, request SDK providers' privacy manifests, and ensure SDK contracts (and their contracts with other third parties) are compatible with the first party's privacy policies.[172]

4.1.7 Data integrity

RECOMMENDATIONS

- Work with experts to anticipate, spot, and correct accuracy and bias issues with data.
- Develop a comprehensive data security program.
- Have procedures in place in the event of a security threat.

Organizations must ensure that their data is accurate, representative, and complete, and that it is protected from unauthorized access and other threats. Organizations should work with experts to anticipate, spot, and correct accuracy and bias issues with their data. They can also conduct algorithmic impact assessments (AIAs), and grant access for independent researchers to test for issues. Organizations can engage with communities who are likely to be affected by their data practices—particularly historically marginalized communities—throughout the product development process. On an individual level, organizations can provide people with opportunities to access, challenge, or delete personal data, in line with data access rights.

New technologies also present opportunities for new cyber attack surfaces that require special attention, particularly if part of critical infrastructure. Hardware and software used in immersive technologies, for example, may be vulnerable to attack by actors seeking to steal sensitive data, surveil users, install malware, or otherwise compromise the user or their devices. Existing cybersecurity frameworks can be adapted to account for unique risks these technologies raise, emphasizing strong user authentication models, PETs, and security and privacy by design and by default practices.[173]

Comprehensive data security programs can help organizations prepare for these challenges. Organizations' chief information security officers, chief technology officers, and other senior security leaders should lead the security program development process. These internal stakeholders should also be involved in coordinating the organization's data practices to ensure they are appropriately secured with technical, administrative, and other safeguards. A comprehensive program should:

- Document data security protocols reflecting current best practices and industry norms.
- Adhere to recognized security frameworks and standards, tailored to the organization's unique risks.
- Regularly engage in threat modeling and vulnerability testing.
- Monitor research for new vulnerabilities and adjust practices accordingly.
- Implement internal controls on employee and contractor access to personal data.

- Conduct ongoing training for organizational staff and any partners.

In the event of a security threat, organizations should have procedures in place to deal with the incident. First and foremost, organizations should ensure compliance with any legal obligations, such as data breach notification laws and regulations.[174] Beyond this, a security incident response plan should include:

- Processes for identifying, managing, and resolving incidents, including when to escalate.
- Clear responsibilities for team members to respond to incidents.
- Remedial actions for responsible parties.
- Periodic review of the incident response process.

4.1.8 Privacy-enhancing technologies (PETs)

RECOMMENDATIONS

- Implement PETs on a case-by-case basis, based on organizational goals and practices.
- Ensure ongoing oversight and monitoring of PETs after they are implemented.

PETs can allow organizations to put body-related data to use while minimizing the privacy risks, and organizations should implement them on a case-by-case basis depending on organizational goals and practices. Organizations should monitor research and technical literature to keep up to date on the latest PETs developments, as well as any vulnerabilities that could threaten their products. In deciding which PETs to adopt, organizations should convene multidisciplinary teams to evaluate how appropriate a given PET would be considering the organization's practices, and weigh any potential tradeoffs between privacy, utility, and any other equities. Potential PETs that may be appropriate for body-related data in immersive environments include:[175]

- **Encryption**: a method to secure data by converting it into a coded format that is readable only with a specific key. Some types of encryption include **end-to-end encryption**, which protects data sent between two parties, and **homomorphic encryption**, which allows an actor to perform computations on the data without breaking the encryption and revealing the data.[176]
- **Differential privacy**: a technique that adds "statistical noise" to a dataset, ensuring that statistical analysis of the dataset doesn't compromise the privacy of individual data entries.[177]
- **Federated learning**: a decentralized machine learning approach in which a model is trained across multiple devices without sharing the data itself.[178] It is similar to **secure multiparty computation**.[179]
- **Synthetic data**: artificially-generated data that mimics real data, and is used for training and testing in privacy-sensitive situations.[180]

Once PETs are implemented, they should be monitored on an ongoing basis, with trained staff checking to make sure that the organization's PETs remain effective over time. Organizations should adapt their PETs strategy to changes in their data practices, technical vulnerabilities and capabilities, and the data ecosystem, as needed.[181]

STAGE 4

Summary of Best Practices

BEST PRACTICE	RECOMMENDATIONS
Data minimization	Implement technical tools such as privacy-enhancing technologies (PETs) and design approaches like privacy by design to put data minimization into practice. Limit exploring new body-related data types and uses to lab and pre-deployment settings, rather than with live user data. Develop internal data retention policies based on how long data must be kept in order to achieve a stated objective or provide a stated service. De-identify or dispose of data once it is no longer needed.
Purpose specification and limitation	Be as specific as possible when identifying data processing purposes. Avoid collecting, using, or transferring data beyond the original stated purposes without additional action.
Transparency: meaningful notice and consent	Provide notice and obtain consent in context, without overwhelming users. Use immersive technologies' unique interface to provide users with more intuitive, effective product and data practice education. Ensure that when users give consent, it is specific, informed, and freely given. Start users with the most privacy-protective default settings and allow them to alter their preferences.
User controls	Allow users to access, correct, and delete their data.
Local and on-device processing and storage	Process and store as much data on a user's device as possible.
Third party management	Conduct due diligence to ensure potential third party data partners abide by compatible privacy policies. Develop and enforce policies by which third parties must comply in order to maintain partnership. Create internal policies regarding transmitting data for research and government requests for data. Limit transmitting data to only what is needed to achieve an objective or provide a service. Explore other technical and organizational tools for third party management.
Data integrity	Work with experts to anticipate, spot, and correct accuracy and bias issues with data. Develop a comprehensive data security program. Have procedures in place in the event of a security threat.
Privacy-enhancing technologies (PETs)	Implement PETs on a case-by-case basis, based on organizational goals and practices. Ensure ongoing oversight and monitoring of PETs after they are implemented.

4.2 Evaluate best practices in regard to one another

Best practices should be implemented together as part of a coherent strategy. At the same time, there may be cases in which best practices conflict with one another or with other organizational priorities. For example, an organization that institutes age assurance techniques to satisfy child safety laws, or to protect children in online spaces, will have to contend with the privacy and equity implications of such practices.[182] Additionally, minimizing data collection about sensitive categories like race, for the purpose of preventing potential discriminatory downstream uses of this data, could foreclose the possibility of collecting data for bias audits.[183] Organizations should consider best practices holistically, balancing tradeoffs and weighing against organizational objectives.

4.3 Assess best practices on an ongoing basis

Once an organization has implemented a robust set of best practices, it is critical to continually monitor and reevaluate as technologies evolve, regulations change, and new data capabilities emerge. Over time, organizations should ask themselves:

- Are the best practices the organization implemented still the preferred practices? Have new practices emerged?
- How have the organization's data practices changed?
- How do any new data practices impact privacy and other organizational equities? Do these practices involve new data types, uses, processing techniques, or partners?
- How has the legal landscape changed, and does this impact the organization's obligations?
- What processes are in place to ensure the organization's policies and procedures continue to be followed?
- What internal expertise does the organization have to ensure it is able to comply with its own policies and procedures?
- If possible, when implementing new data practices, does the organization have access to a regulatory sandbox in which it could do so under the supervision of a regulator?[184]

CONCLUSION

This framework serves as a starting point for organizations that collect, use, or transfer body-related data to develop best practices that prioritize user privacy. It is particularly relevant in the context of immersive technologies, but is applicable in other environments that involve body-related data as well. As technologies become more immersive, the unique considerations raised in this framework will be relevant for a growing number of organizations and the virtual experiences they create. Organizations can use this framework as a guide as they examine, develop, and refine their data practices. Ultimately, decisions about these practices will need to be made by each organization on a case-by-case basis. As technologies evolve, and as the regulatory landscape changes, organizations need to ensure their data practices not only maintain legal compliance, but protect people's privacy.

Appendix A: Relevant Existing U.S. Privacy Laws

TYPE OF LAW	LAW
Comprehensive data privacy laws	California Consumer Privacy Act/California Privacy Rights Act (CCPA/CPRA)[185]
	Colorado Privacy Act (CPA)[186]
	Connecticut Data Privacy Act (CTDPA)[187]
	Delaware Personal Data Privacy Act (DPDPA)[188]
	Florida Digital Bill of Rights (FDBR)[189]
	Indiana Consumer Data Protection Act (INCDPA)[190]
	Iowa Consumer Data Protection Act (ICDPA)[191]
	Montana Consumer Data Privacy Act (MTCDPA)[192]
	Oregon Consumer Privacy Act (OCPA)[193]
	Tennessee Information Protection Act (TIPA)[194]
	Texas Data Privacy and Security Act (TDPSA)[195]
	Utah Consumer Privacy Act (UCPA)[196]
	Virginia Consumer Data Protection Act (VCDPA)[197]
Biometric privacy laws and policy statements	Illinois Biometric Privacy Act (BIPA)[198]
	Texas Capture and Use of Biometric Identifier Act (CUBI)[199]
	Washington Biometric Privacy Protection Act (BPPA)[200]
	Education-focused biometric laws[201]
Youth privacy	Children's Online Privacy Protection Act (COPPA)[202]
Unfair and deceptive practices	FTC Act Section 5[203]
Health data privacy laws	Health Insurance Portability and Accountability Act (HIPAA)[204]
	Washington My Health My Data Act (MHMD)[205]
	Nevada S.B. 370[206]

Appendix B: XR Data Flows Illustration

Appendix C: Risk Framework Worksheet

Organizations can use the following worksheet to document and track their progress through the risk framework, recording any relevant notes in the right column.

I. UNDERSTANDING HOW ORGANIZATIONS USE PERSONAL DATA		
Create data maps		
Be able to explain the purpose of each data practice		
Identify all relevant data stakeholders	Third-party recipients of data:	Data subjects and other impacted people:

II. ANALYZING RELEVANT LEGAL FRAMEWORKS AND ENSURING COMPLIANCE		
Understand existing legal obligations	Data types covered under existing privacy laws (personal, biometric, sensitive, health, publicly available):	
	Consumer rights under existing privacy laws:	Business obligations under existing privacy laws:
Understand the changing legal landscape		

III. IDENTIFYING AND ASSESSING RISKS TO INDIVIDUALS, COMMUNITIES, AND SOCIETY	
Identify risks related to data type	Identifiability:
	Sensitivity:
	Potential for inferences:
	Data accuracy and bias:

Appendix C: Risk Framework Worksheet *(continued)*

III. IDENTIFYING AND ASSESSING RISKS TO INDIVIDUALS, COMMUNITIES, AND SOCIETY	
Identify risks related to data handling	Critical decisions:
	Partners and third parties:
	Data retention:
	User expectations and understanding:
Assess fairness, ethics, and responsibility	

IV. IMPLEMENTING RELEVANT BEST PRACTICES	
Implement best practices	Data minimization:
	Purpose specification and limitation:
	Transparency: meaningful notice and consent:
	User controls:
	Local and on-device processing and storage:
	Third party management:
	Data integrity:
	Privacy-enhancing technologies (PETs):
Evaluate best practices with regard to one another	
Assess best practices on an ongoing basis	

Endnotes

1 "Immersive technologies" refers to a collection of hardware and software products that substitute, enhance, or alter users' individual, physical-world experiences. As used in this report, it does not refer to a discrete, static set of technologies, though common immersive technologies include extended reality (XR), virtual worlds, gaming platforms, and brain-computer interfaces. Closely related concepts also include "ambient intelligence/computing," "spatial computing," and "the metaverse."

A few examples include: Henry Wilhelm and Tomas Kellner, *Amazon is Making Your Life Easier Through Ambient Intelligence*, About Amazon (Oct. 5, 2022), https://www.aboutamazon.com/news/devices/amazon-is-making-your-life-easier-through-ambient-intelligence; Hector Ouilhet, *More Human Ambiance in Ambient Computing,* Google Design (Nov. 12, 2020), https://design.google/library/more-human-ambiance-in-ambient-computing; *Introducing Apple Vision Pro: Apple's First Spatial Computer*, Apple Newsroom (June 5, 2023), https://www.apple.com/newsroom/2023/06/introducing-apple-vision-pro/; *Learn About Who We Are*, Meta, https://about.meta.com/metaverse.

2 This report uses the term "data practice" to refer to any action an organization takes involving the collection, use, or transferring of data.

3 Daniel Berrick and Jameson Spivack, *Understanding Extended Reality Technology & Data Flows: XR Functions*, Future of Privacy Forum (Oct. 31, 2022), https://fpf.org/blog/understanding-extended-reality-technology-data-flows-xr-functions/.

4 Daniel Berrick and Jameson Spivack, *Understanding Extended Reality Technology & Data Flows: Privacy and Data Protection Risks and Mitigation Strategies*, Future of Privacy Forum (Nov. 17, 2022), https://fpf.org/blog/understanding-extended-reality-technology-data-flows-privacy-and-data-protection-risks-and-mitigation-strategies/.

5 Mark McGill, *Extended Reality (XR) and the Erosion of Anonymity and Privacy*, IEEE (Nov. 18, 2021), https://standards.ieee.org/wp-content/uploads/import/governance/iccom/extended-reality-anonymity-privacy.pdf.

6 *Id.*

7 For example, organizations that collect voice data for smart home devices or virtual assistants.

8 *Data Mapping: All You Need to Know*, Ethyca, https://ethyca.com/about-data-mapping.

9 As defined in the European Union (EU)'s General Data Protection Regulation (GDPR), "personal data" is defined as "any information which [is] related to an identified or identifiable natural person." Regulation (EU) 2016/679 Art. 4, https://gdpr.eu/article-4-definitions/.

10 *Data Mapping Automation*, OneTrust, https://www.onetrust.com/products/data-mapping-automation/.

11 *GDPR Data Mapping: What It Is and How to Comply?*, Securiti (June 26, 2023), https://securiti.ai/blog/gdpr-data-mapping/.

Controllers with 250+ employees must maintain records of processing activities. Regulation (EU) 2016/679 Art. 30, https://gdpr.eu/article-30-records-of-processing-activities/.

DPIAs are required if the process or technology is likely to result in a "high risk" to human rights and freedoms. Regulation (EU) 2016/679 Art. 35, https://gdpr.eu/article-35-impact-assessment/.

12 *What is the Difference Between 3DoF vs 6DoF in VR? The Comprehensive Guide to Degrees of Freedom*, Smart VR Lab (Mar. 4, 2021), https://www.smartvrlab.nl/3dof-vs-6dof-in-vr/.

13 There are also tools for organizations to manage their data lakes, including privacy and security issues. *Introduction to Data Lakes*, Databricks, https://www.databricks.com/discover/data-lakes.

14 *Fair Information Practice Principles (FIPPs),* Federal Privacy Council*,* https://www.fpc.gov/resources/fipps/.

15 "Privacy leaders collect data and use metrics to measure, assess, and improve the performance of their privacy programs. Beyond demonstrating compliance, privacy metrics have emerged as key to measure and improve privacy program performance and maturity in terms of customer trust, risk mitigation, and business enablement. Privacy leaders use metrics to benchmark the maturity of their organization's privacy program against its strategy and goals and demonstrate how privacy contributes to its strategy and bottom line." Omer Tene and Mary Culnan, *Privacy Metrics Report*, Future of Privacy Forum (Sep. 2021), https://fpf.org/wp-content/uploads/2022/03/FPF-PrivacyMetricsReport-R9-Digital.pdf.

16 "Prior to the introduction of this framework, there was a tendency among the participating companies to opt for collecting all available data types in their proposed use cases. By considering the benefits to both the user and the business, participants were able to balance their hopes of future monetization against the risks of driving people away through excessive data collection. Particularly with emerging and novel technology, people will err on the side of caution, moving away from products they perceive as having unjustified data collection practices. We found this template was particularly useful in assisting companies to clearly articulate the value of data processing and rationalize their collection practices. This led to discussions around privacy-centered alternatives using less sensitive inputs." *Data Transparency and Control in XR and the Metaverse*, Meta Trust, Transparency & Control Labs (June 2023), https://www.ttclabs.net/site/assets/files/11085/data_transparency_and_control_in_xr_and_the_metaverse_report.pdf.

17 For example, in the EU, the GDPR requires a legal basis for each processing activity, including consent, performance of a contract, legitimate interest, vital interest, legal requirement, and/or public interest. Regulation (EU) 2016/679 Art. 6, https://gdpr.eu/article-6-how-to-process-personal-data-legally/.

18 The Input > Use > Value Template was developed by Meta Trust, Transparency & Control Labs as part of a co-design session conducted in Singapore in collaboration with the Singapore Infocomm Media Development Authority and Personal Data Protection Commission. *Data Transparency and Control in XR and the Metaverse*, Meta Trust, Transparency & Control Labs (June 2023), https://www.ttclabs.net/site/assets/files/11085/data_transparency_and_control_in_xr_and_the_metaverse_report.pdf.

19 Joseph O'Hagan, Pejman Saeghe, et al., *Privacy-Enhancing Technology and Everyday Augmented Reality: Understanding Bystanders' Varying Needs for Awareness and Consent*, Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (Jan. 11, 2023), https://dl.acm.org/doi/10.1145/3569501.

20 Solon Barocas and Andrew D. Selbst, *Big Data's Disparate Impact*, California Law Review (Sep. 30, 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899.

21 Comprehensive privacy laws differ from narrower privacy laws in that they apply to multiple sectors. In definitions of "personal data," comprehensive laws may also include inferences. For example, the California Consumer Privacy Act/California Privacy Rights Act (CCPA/CPRA) defines "personal data" to include "[i]nferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes." Cal. Civ. Code §§ 1798.100 to 1798.199, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

22 The CCPA/CPRA contains a broad definition of personal data, which includes biometric information. Cal. Civ. Code §§ 1798.100 to 1798.199, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

Illinois' Biometric Privacy Act (BIPA) also applies to biometric information, although its scope is limited to this kind of data rather than personal data more broadly. 740 Ill. Comp. Stat. Ann. §§ 14/1 to 14/25, https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

23 Tatiana Rice, *When is a Biometric No Longer a Biometric*?, Future of Privacy Forum (May 19, 2022), https://fpf.org/blog/when-is-a-biometric-no-longer-a-biometric/.

24 *New Study Exposes Impact of Illinois Biometric Privacy Law*, Chamber of Progress (Apr. 5, 2023), https://progresschamber.org/new-study-exposes-impact-of-illinois-biometric-privacy-law/.

25 Florida law prohibits agencies and institutions from collecting, obtaining, or retaining "biometric information of a student or a parent or sibling of the student." Fla. Stat. § 1002.222, https://www.flsenate.gov/Laws/Statutes/2023/1002.222.

26 Texas and Washington have enacted biometric data privacy laws: the Texas Capture and Use of Biometric Identifier Act (CUBI), and the Washington Biometric Privacy Protection Act (BPPA).

27 Jameson Spivack, Tatiana Rice, et al., *Old Laws & New Tech: As Courts Wrestle With Tough Questions Under U.S. Biometric Laws, Immersive Tech Raises New Challenges*, Future of Privacy Forum (July 27, 2023), https://fpf.org/blog/old-laws-new-tech-as-courts-wrestle-with-tough-questions-under-us-biometric-laws-immersive-tech-raises-new-challenges/.

28 In *Theriot v. Louis Vuitton North America, Inc.*, a BIPA claim was permitted to proceed against Louis Vuitton's virtual try-on (VTO) sunglasses app, finding that the VTO technology's use of facial scans was analogous to BIPA case law, which held that face scans derived from photographs constitute biometric identifiers. *Theriot v. Louis Vuitton North America, Inc.*, Case No. 1:22 CV 02944 (S.D.N.Y. filed Dec. 5, 2022), https://law.justia.com/cases/federal/district-courts/new-york/nysdce/1:2022cv02944/578061/36/.

29 Organizations should determine whether body-related data is legally "sensitive" even if it does not qualify as a biometric, since this information can reveal or be used to infer sensitive characteristics that receive heightened protection.

30 Kaitlyn Harger, *Who Benefits From BIPA? An Analysis of Cases Brought Under Illinois' State Biometrics Law*, Chamber of Progress (Apr. 2023), https://progresschamber.org/wp-content/uploads/2023/03/Who-Benefits-from-BIPA-Analysis-of-Cases-Under-IL-Biometrics-Law.pdf.

31 In addition to the inferences themselves, non-sensitive data from which sensitive inferences are drawn may also be sensitive under U.S. data privacy laws such as the Colorado Privacy Act (CPA). Colo. Rev. Stat. §§ 6-1-1301 to 6-1-1313, https://law.justia.com/codes/colorado/2022/title-6/article-1/part-13/.

For more on the application of sensitive data definitions to inferences and the data used to make them, *see* Daniel Solove, *Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data*, Northwestern University Law Review (Jan. 11, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4322198.

32 Vivek Nair, Christian Rack, et al., *Inferring Private Personal Attributes of Virtual Reality Users from Head and Hand Motion Data*, arXiv (June 10, 2023), https://arxiv.org/pdf/2305.19198.pdf.

33 Daniel Berrick, *BCI Commercial and Government Use: Gaming, Education, Employment, and More*, Future of Privacy Forum (Feb. 8, 2022), https://fpf.org/blog/bci-commercial-and-government-use-gaming-education-employment-and-more/.

34 *E.g.*, Connecticut Personal Data Privacy Act (CTDPA). Conn. Gen. Stat. §§ 42-515 to 42-525, https://portal.ct.gov/AG/Sections/Privacy/The-Connecticut-Data-Privacy-Act.

35 The CCPA/CPRA and CTDPA illustrate the importance of consent, requiring organizations to provide individuals opt-out rights, including the right to opt out of data sales and other transfers when processing sensitive data.

36 For example, the majority of comprehensive state privacy laws classify children's personal data as sensitive, but this data is not considered sensitive under the CCPA/CPRA and the Utah Consumer Privacy Act (UCPA).

37 For how the GDPR applies to sensitive data, *see* Regulation (EU) 2016/679 Art. 9, https://gdpr.eu/article-9-processing-special-categories-of-personal-data-prohibited/.

38 *Understanding Eye Tracking & How it Can Work for You: Definitions, Metrics, and Applications*, Eyeware (Mar. 3, 2022), https://eyeware.tech/blog/what-is-eye-tracking/.

39 Vivek Nair, Gonalo Munilla-Garrido, et al., *Exploring the Privacy Risks of Adversarial VR Game Design*, arXiv (Jul. 17, 2023), https://arxiv.org/pdf/2207.13176.pdf.

While some conditions and diseases are observable to a human and possibly an algorithm, others require large quantities of body-related data and analysis to uncover. Linda Roach, *How AI Learns to Detect Diabetic Eye Disease*, EyeNet Magazine (Feb. 2017), https://www.aao.org/eyenet/article/how-ai-learns-to-detect-diabetic-eye-disease.

Daniel Berrick and Jameson Spivack, *Understanding Extended Reality Technology & Data Flows: Privacy and Data Protection Risks and Mitigation Strategies*, Future of Privacy Forum (Nov. 17, 2022),

https://fpf.org/blog/understanding-extended-reality-technology-data-flows-privacy-and-data-protection-risks-and-mitigation-strategies/.

40 Mike Hintze, *The Washington My Health My Data Act - Part 1: An Overview*, Hintze Law (Apr. 10, 2023), https://hintzelaw.com/hintzelaw-blog/2023/4/9/wa-my-health-my-data-act-pt1-overview.

41 Va. Code Ann. §§ 59.1-575 to 59.1-584, https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/.

42 *U.S. State Privacy Legislation Tracker*, IAPP (Nov. 10, 2023), https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf.

43 The Delaware Personal Data Privacy Act (DPDPA) also has a broader deletion right than other state data privacy laws, applying to data obtained about a person from a third-party source in addition to that directly obtained from the individual. 84 Del. Laws §§ 12D-101 to 12D-111, https://www.legis.delaware.gov/BillDetail?legislationId=140388.

44 For example, controllers are required to obtain a consumer's affirmative consent for processing adolescent data for targeted advertising and sales in Connecticut, but not in Iowa and Indiana. Conn. Gen. Stat. §§ 42-515 to 42-525, https://portal.ct.gov/AG/Sections/Privacy/The-Connecticut-Data-Privacy-Act; Iowa Code §§ 715D.1 to 715D.9, https://casetext.com/statute/code-of-iowa/title-xvi-criminal-law-and-procedure/chapter-715d; Ind. Code §§ 24-15-1-1 to 24-15-11-2, https://iga.in.gov/legislative/2023/bills/senate/5/details.

Some laws require opt-in consent, while others only require companies to provide individuals with a mechanism for opting out of processing body-related data. *Comparison of Indiana, Iowa & Connecticut Privacy Frameworks*, Future of Privacy Forum (Apr. 2023), https://fpf.org/wp-content/uploads/2023/04/IN-CT-and-IA-Comparison-Chart-FINAL.pdf.

45 *E.g.*, The CPA Rule 7.03(F) notes that an "agreement obtained through dark patterns" does not constitute consent. Colo. Code Regs. § 904-3-7.03(F), https://coag.gov/app/uploads/2022/10/CPA_Final-Draft-Rules-9.29.22.pdf.

For the Federal Trade Commission (FTC)'s guidance on "dark patterns," *see Bringing Dark Patterns to Light*, FTC (Sep. 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.

46 *Metaverse Privacy and Safety*, World Economic Forum (July 2023), https://www3.weforum.org/docs/WEF_Metaverse_Privacy_and_Safety_2023.pdf.

47 DPIAs are a way for companies to document processing activities, assess associated harms or risks of harm, and identify measures for mitigating or preventing harms. *Data protection impact assessments*, Information Commissioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-impact-assessments/.

48 Daniel Berrick and Jameson Spivack, *Understanding Extended Reality Technology & Data Flows: Privacy and Data Protection Risks and Mitigation Strategies*, Future of Privacy Forum (Nov. 17, 2022), https://fpf.org/blog/understanding-extended-reality-technology-data-flows-privacy-and-data-protection-risks-and-mitigation-strategies/.

Adam Satariano and Paul Mozur, *The People Onscreen Are Fake. The Disinformation Is Real.*, The New York Times (Feb. 7, 2023),

https://www.nytimes.com/2023/02/07/technology/artificial-intelligence-training-deepfake.html.

Karen Kornbluh, *Disinformation, Radicalization, and Algorithmic Amplification: What Steps Can Congress Take?*, Just Security (Feb. 7, 2022),

https://www.justsecurity.org/79995/disinformation-radicalization-and-algorithmic-amplification-what-steps-can-congress-take/.

49 For example, the CPA lists activities that pose a "heightened risk of harm" to consumers, such as selling personal data and processing sensitive data, while Connecticut's SB 3, which amends the CTDPA, includes deceptive treatment, intrusion upon seclusion, and reputational injury in defining "heightened risk of harm." Colo. Code Regs. § 904-3-2.02, https://coag.gov/app/uploads/2022/10/CPA_Final-Draft-Rules-9.29.22.pdf.

Conn. S.B. 3 § 8(5) (2023), https://www.cga.ct.gov/asp/CGABillStatus/cgabillstatus.asp?selBillType=Bill&bill_num=SB3.

California Age-Appropriate Design Code Act, Cal. Civ. Code §§ 1798.99.28 to 1798.99.40,

https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=202120220AB2273&showamends=false.

50 While not specifically targeted towards youth privacy, state comprehensive data privacy laws also have provisions addressing youth privacy. For example, the comprehensive privacy laws in Delaware, California, Connecticut, and Montana prohibit covered entities from selling or processing, for targeted advertising purposes, the data of consumers that they know, or willfully disregard, are between certain ages.

51 The FTC has articulated an expansive view of "biometric" data in the COPPA context, covering body-related data that identifies an individual, can be used to identify an individual, or is reasonably linked to an individual's profile or ID. In case law, the Commission has explicitly stated that many body-related data types common in immersive technologies, such as eye tracking, are considered biometric data. These broad interpretations of "biometric" data likely mean that nearly all body-related data immersive technologies collect will be regulated as "personal information" under COPPA. *Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act*, *FTC* (May 18, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf.

FTC v. Microsoft, Case No. 2:23-CV-00836 (W.D. Wash. filed Jun. 5, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/microsoftproposedstiporder.pdf.

52 Some immersive technologies process data on devices for privacy purposes and to boost performance. It is unclear whether on-device processing is considered collection under COPPA, the absence of which would take the processing outside of the law's scope.

53 Additionally, the FTC has not updated the COPPA rule since 2013.

54 *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FTC (May 2021), https://www.ftc.gov/about-ftc/mission/enforcement-authority.

55 In 2023, a major trend in privacy laws was a focus on children and teens. For example, the Kids Online Safety Act (KOSA), if passed, would require certain entities, including those that act as "virtual reality environments," to make public reports that identify foreseeable risk of harm to minors, and the measures the entity has taken to address them. Kids Online Safety Act, S. 3663, 118th Cong. (2023), https://www.congress.gov/bill/117th-congress/senate-bill/3663/text.

56 The broad scope of Washington's My Health My Data Act (MHMD) and other similar bills indicates that many types of body-related data, even those not typically labeled health data by data privacy laws, may fall within the definition of "consumer health data." For example, a 2023 legislative proposal in Maine defined "consumer health data" as "personal information that describes or reveals the past, present or future physical health, mental health, disability, diagnosis or health condition of a consumer." If consumer health privacy proposals gain traction, organizations may need to apply compliance obligations to a growing amount of body-related data. Maine My Health My Data Act, H.B. 1902 (2023), http://www.mainelegislature.org/legis/bills/getPDF.asp?paper=HP1217&item=1&snum=131.

57 For example, *Netchoice v. Bonta* found that several provisions of the California AADC violated the First Amendment, raising the likelihood that similar "design-code" style efforts might encounter constitutional challenges. *NetChoice v. Rob Bonta*, Case No. 5:22-CV-08861 (N.D. Cal. filed Sep. 18, 2023), https://netchoice.org/wp-content/uploads/2023/09/NETCHOICE-v-BONTA-PRELIMINARY-INJUNCTION-GRANTED.pdf.

Regarding biometric data, BIPA's private right of action has led to numerous lawsuits addressing the meaning of "biometric" data and the obligations it entails. *New Study Exposes Impact of Illinois Biometric Privacy Law*, Chamber of Progress (Apr. 5, 2023), https://progresschamber.org/new-study-exposes-impact-of-illinois-biometric-privacy-law/.

These cases demonstrate that at least some body-related data will be considered "biometric" data—even data that organizations neither actively use nor plan to use for identification. Jameson Spivack, Tatiana Rice, et al., *Old Laws & New Tech: As Courts Wrestle With Tough Questions Under U.S. Biometric Laws, Immersive Tech Raises New Challenges*, Future of Privacy Forum (July 27, 2023), https://fpf.org/blog/old-laws-new-tech-as-courts-wrestle-with-tough-questions-under-us-biometric-laws-immersive-tech-raises-new-challenges/.

However, the exact overlap between biometrics and body-related data will continue to evolve through BIPA adjudication and other biometric law enforcement. While BIPA litigation has provided the most insight into how courts interpret this question, organizations should also monitor developments in Texas and Washington, which also have biometric privacy laws. *E.g.*, *The State of Texas vs. Meta Platforms Inc. f/k/a Facebook*, Cause No. 22-0121 (Tex. 71st Jud. Dist filed Feb. 14, 2022), https://texasattorneygeneral.gov/sites/default/files/images/child-support/State%20of%20Texas%20v.%20Meta%20Platforms%20Inc..pdf.

58 This framework takes a broad, open-ended view of the terms "fair," "ethical," and "responsible," recognizing that there is no consensus on their definitions. In this section, "fair" is not used in the legal sense, as it is in the context of "unfair or deceptive acts or practices," a key component of the U.S. consumer protection regulations such as the FTC Act, or the GDPR Article 5's requirement that personal data be processed "fairly."

59 For example, disclosing health-related data to law enforcement may raise risks for individuals in jurisdictions that have criminalized abortion.

60 Paul Ohm, *Sensitive Information*, Southern California Law Review (Jan. 2018), https://southerncalifornialawreview.com/wp-content/uploads/2018/01/88_1125.pdf.

61 Daniel Solove, *Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data*, Northwestern University Law Review (Jan. 11, 2023), https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2923&context=faculty_publications.

62 Brittan Heller, *Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law*, Vanderbilt Journal of Entertainment and Technology Law (2020), https://scholarship.law.vanderbilt.edu/jetlaw/vol23/iss1/1/.

63 Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, Northwestern University Law Review (Oct. 9, 2022), https://scholarlycommons.law.northwestern.edu/nulr/vol117/iss2/1/.

64 Daniel Solove, *Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data*, Northwestern University Law Review (Jan. 11, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4322198.

65 Tatiana Rice, *When is a Biometric No Longer a Biometric?*, Future of Privacy Forum (May 19, 2022), https://fpf.org/blog/when-is-a-biometric-no-longer-a-biometric/.

66 Patrick Grother, Mei Ngan, et al., *Face Recognition Technology Evaluation (FRTE) Part 1: Verification*, National Institute of Standards and Technology (Nov. 21, 2023), https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf.

67 Vivek Nair, Wenbo Guo, et al., *Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data*, arXiv (Feb. 17, 2023), https://arxiv.org/abs/2302.08927.

68 *See* "Stage 4: Implementing Relevant Best Practices."

69 Simson L. Garfinkel, *De-Identification of Personal Information*, National Institute of Standards and Technology (Oct. 2015), https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf?uuid=n2tDjSm0DpcTq02f5027.

70 For example, disclosure of the fact that an individual has a fatal disease may cause embarrassment or make it more difficult to get a job or loan. Daniel Solove, *Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data*, Northwestern University Law Review (Jan. 11, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4322198.

71 *See* "Stage 2: Analyzing Relevant Legal Frameworks and Ensuring Compliance." *See also* Daniel Solove, *Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data*, Northwestern University Law Review (Jan. 11, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4322198.

72 Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, Northwestern University Law Review (Oct. 9, 2022), https://scholarlycommons.law.northwestern.edu/nulr/vol117/iss2/1/.

73 Daniel Solove, *Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data*, Northwestern University Law Review (Jan. 11, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4322198.

74 Vivek Nair, Gonalo Munilla-Garrido, et al., *Exploring the Privacy Risks of Adversarial VR Game Design*, arXiv (July 17, 2023), https://petsymposium.org/2023/files/papers/issue4/popets-2023-0108.pdf.

75 Colo. Code Regs. § 904-3-2.02, https://coag.gov/app/uploads/2022/10/CPA_Final-Draft-Rules-9.29.22.pdf.

76 For more on how data commonly collected in immersive environments can be used to infer sensitive data, and/or harm users, *see* Vivek Nair, Gonalo Munilla-Garrido, et al., *Exploring the Unprecedented Privacy Risks of the Metaverse*, arXiv (July 17, 2023), https://arxiv.org/abs/2207.13176.

77 For information on immersive tech in education, *see Education in XR*, XR Association (May 2023), https://xra.org/wp-content/uploads/2023/05/XRA_Slicks_Education_V1.pdf-1.pdf.

For healthcare, *see XR Technology and Healthcare*, XR Association (May 2023), https://xra.org/wp-content/uploads/2023/05/XRA_Slicks_Healthcare_V2.pdf-1.pdf.

For manufacturing, *see* XR Technology and Manufacturing, XR Association (May 2023), https://xra.org/wp-content/uploads/2023/05/XRA_Slicks_Manufacturing_V1-1.pdf-1-1.pdf.

78 Health Insurance Portability and Accountability Act (HIPAA), *Health Information Privacy*, 42 U.S.C. § 1301 *et seq*., https://www.cdc.gov/phlp/publications/topic/hipaa.html.

79 Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g, https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

80 Helen Nissenbum, *Privacy as Contextual Integrity*, Washington Law Review (2004), https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/.

81 Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, Northwestern University Law Review (Oct. 9, 2022), https://scholarlycommons.law.northwestern.edu/nulr/vol117/iss2/1/.

82 Jameson Spivack, *Cop Out: Automation in the Criminal Legal System*, Center on Privacy & Technology at Georgetown Law (Mar. 29, 2023), https://copout.tech/.

83 Vivek Nair, Gonalo Munilla-Garrido, et al., *Exploring the Privacy Risks of Adversarial VR Game Design*, arXiv (July 17, 2023), https://petsymposium.org/2023/files/papers/issue4/popets-2023-0108.pdf.

84 Brittan Heller, *Reimagining Reality: Human Rights and Immersive Technology*, Carr Center For Human Rights Policy, Harvard Kennedy School (June 12, 2020), https://carrcenter.hks.harvard.edu/files/cchr/files/ccdp_2020-008_brittanheller.pdf.

85 *Id.*

86 Kent Bye, *Biometric Data Streams & the Unknown Ethical Threshold of Predicting & Controlling Behavior*, Voices of VR (Mar. 20, 2017), https://voicesofvr.com/517-biometric-data-streams-the-unknown-ethical-threshold-of-predicting-controlling-behavior/.

87 For example, face analysis trained primarily on younger, lighter-skinned male faces will be biased by age, race, and gender, working more accurately on people demographically similar to those it was trained on. Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research, Conference on Fairness, Accountability, and Transparency (Feb. 2018), https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

88 *See* Elisa Jillson, *Aiming for Truth, Fairness, and Equity in Your Company's Use of AI*, FTC (Apr. 19, 2021), https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai.

Michael Atleson, *Keep Your AI Claims in Check*, FTC (Feb. 27, 2023), https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check.

Michael Atleson, *The Luring Test: AI and the Engineering of Consumer Trust*, FTC (May 1, 2023), https://www.ftc.gov/business-guidance/blog/2023/05/luring-test-ai-engineering-consumer-trust.

Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems, FTC, https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf.

89 Maria de Marisco and Alessio Mecca, *A Survey on Gait Recognition via Wearable Sensors*, ACM Computing Surveys (Aug. 2019), https://dl.acm.org/doi/pdf/10.1145/3340293.

90 The form factor used to collect and process data will also impact accuracy. A limitation for consumer products is that the form factor typically needs to be small, low-cost, and portable, potentially limiting its computing power. *See id. See also A Survey on Gait Recognition via Wearable Sensors*, ACM Computing Surveys (Aug. 2019), https://dl.acm.org/doi/pdf/10.1145/3340293.

91 Nicol Turner Lee, *Detecting Racial Bias in Algorithms and Machine Learning*, Journal of Information, Communication and Ethics in Society (Aug. 13, 2018), https://www.emerald.com/insight/content/doi/10.1108/JICES-06-2018-0056/full/html.

92 Olga Akselrod and Jacob Snow, *California's Court of Appeals Rules that Meta Can't Evade Liability in Case Claiming Facebook's Ad Tools Violate Users' Civil Rights*, ACLU (Sept. 25, 2023), https://www.aclu.org/press-releases/californias-court-of-appeals-rules-that-meta-cant-evade-liability-in-case-claiming-facebooks-ad-tools-violate-users-civil-rights.

93 For more, *see* "Stage 4: Implementing Relevant Best Practices."

94 For more on the tension between improving accuracy/eliminating bias and data minimization in AI, *see* Andrew Burt and Brenda Leong, *AI vs. Privacy: How to Reconcile the Need for Sensitive Data with the Principle of Minimization*, IAPP (Aug. 16, 2023), https://iapp.org/news/a/ai-vs-privacy-how-to-reconcile-the-need-for-sensitive-data-with-the-principle-of-minimization/.

95 *Big Data: A Tool for Inclusion or Exclusion?*, FTC Report (Jan. 2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

96 *See* Solon Barocas and Andrew D. Selbst, *Big Data's Disparate Impact*, California Law Review (June 2016), https://www.jstor.org/stable/24758720. *See also Unfairness by Algorithm: Distilling the Harms of Automated Decision-Making*, Future of Privacy Forum (Dec. 2017), https://fpf.org/blog/unfairness-by-algorithm-distilling-the-harms-of-automated-decision-making/.

97 Jinyan Zang, *Solving the Problem of Racially Discriminatory Advertising on Facebook*, Brookings (Oct. 19, 2021), https://www.brookings.edu/articles/solving-the-problem-of-racially-discriminatory-advertising-on-facebook/.

98 The FTC's policy statement on biometric information and unfair/deceptive acts/practices addresses this potential for biometric information. *Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act*, FTC (May 18, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf.

99 Connie Chen, *All the New Amazon Devices and Features Coming Soon to Your Home, Including Pre-Order Details*, Amazon (Sept. 20, 2023), https://www.aboutamazon.com/news/devices/amazon-fall-event-2023-announcements.

Meta Connect, Meta (2023), https://www.metaconnect.com/en/home.

Daniel Sturman, *Generative AI on Roblox: Our Vision for the Future of Creation*, Roblox (Feb. 17, 2023), https://blog.roblox.com/2023/02/generative-ai-roblox-vision-future-creation/.

Matthew DeHamer, *Three Ways Our AI is Powering Awe-Inspiring XR Experiences*, Qualcomm (May 17, 2023), https://www.qualcomm.com/news/onq/2023/05/three-ways-our-ai-is-powering-awe-inspiring-xr-experiences.

100 Jameson Spivack and Daniel Berrick, *Immersive Tech Obscures Reality. AI Will Threaten It*, WIRED (Sept. 27, 2023), https://www.wired.com/story/immersive-technology-artificial-intelligence-disinformation/.

101 Louis Rosenberg, *Why Generative AI is More Dangerous than You Think*, Venture Beat (May 6, 2023), https://venturebeat.com/ai/why-generative-ai-is-more-dangerous-than-you-think/.

102 *Best Practices for AI and Workplace Assessment Technologies*, Future of Privacy Forum (Sept. 2023), https://fpf.org/wp-content/uploads/2023/09/FPF-Best-Practices-for-AI-and-HR-Final.pdf.

103 Vivek Nair, Gonzalo Munilla Garrido, et al., *Exploring the Unprecedented Privacy Risks of the Metaverse*, arXiv (July 2022), https://arxiv.org/abs/2207.13176.

104 If so, Children's Online Privacy Protection Act (COPPA) compliance obligations will apply. *See Complying with COPPA: Frequently Asked Questions*, FTC (July 2020), https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions.

105 For example, students are protected by FERPA. 20 U.S.C. § 1232g, https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

106 For example, disclosing health-related data to law enforcement may raise risks for individuals in jurisdictions that have criminalized abortion. Other third parties that might pose heightened risk include foreign adversaries or political actors.

107 SDKs raise risks, in part, because both providers and their third-party contractors may lack transparency about their practices. These practices could include overcollection of user data or unanticipated uses of this data. Daniel Goldberg and Rick Borden, *Regulators and Litigators are Investigating Data Flows Through SDKs – An Overview and Practical Steps to Reduce Risk*, Frankfurt Kurnit Klein & Selz (Aug. 23, 2023), https://technologylaw.fkks.com/post/102imku/regulators-and-litigators-are-investigating-data-flows-through-sdks-an-overview.

108 For example, harm could result from first- or third-party data misuse, or from a cybersecurity incident that exposes user data.

109 Alexandre Gonfalonieri, *Why Machine Learning Models Degrade In Production*, Medium (Jul. 25, 2019), https://towardsdatascience.com/why-machine-learning-models-degrade-in-production-d0f2108e9214.

110 For example, some laws require organizations to keep data for a certain period of time for the purposes of auditing or granting data access rights.

111 Helen Nissenbaum, *Symposium: Privacy as Contextual Integrity*, Washington Law Review (2004), https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/.

112 Ellysse Dick, *Balancing User Privacy and Innovation in Augmented and Virtual Reality*, Information Technology & Innovation Foundation (Mar. 4, 2021), https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality/.

113 Arielle Feger, *In the Game of Trust, Consumers Value Data Transparency Over Liking a Product or Service*, Insider Intelligence (May 9, 2023), https://www.insiderintelligence.com/content/game-of-trust-consumers-value-data-transparency-over-liking-product-service.

114 Lee Rainie and Maeve Duggan, *Privacy and Information Sharing*, Pew Research Center (Jan. 14, 2016), https://www.pewresearch.org/internet/2016/01/14/privacy-and-information-sharing/.

115 Martin Abrams, *The Origins of Personal Data and Its Implications for Governance*, The Information Accountability Foundation (Mar. 21, 2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2510927.

XR data can be broadly categorized as: "observable" (data that XR technologies and third parties can observe and replicate); "observed" (data that individuals provide or generate, third parties can observe but not replicate); "computed" (inferred data); or "associated" (data that on its own does not provide descriptive details about a person). Ellysse Dick, *Balancing User Privacy and Innovation in Augmented and Virtual Reality*, Information Technology & Innovation Foundation (Mar. 4, 2021), https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality/.

116 Specific privacy laws also dictate what kind of information must be included in privacy notices and how. Organizations should ensure their notices are compliant with these requirements.

117 Additionally, these types of notice and consent are difficult to implement effectively for screenless technologies such as Internet of Things devices and voice-based interfaces. *Redesigning Data Privacy:*

Reimagining Notice & Consent for Human-Technology Interaction, World Economic Forum (July 2020), https://www3.weforum.org/docs/WEF_Redesigning_Data_Privacy_Report_2020.pdf.

118 As challenging as implementing notice and consent in immersive technologies is, it may also be an opportunity to improve the paradigm overall. For instance, it might be possible to design more kinetic notice and consent practices that are more intuitive, and more informative, in immersive environments. *See* Evan Selinger, Ely Altman, et al., *Eye-Tracking in Virtual Reality*, Privacy Studies Journal (Mar. 24, 2023), https://tidsskrift.dk/privacy_studies_journal/article/view/134656.

119 Sebastião Barros Vale and Daniel Berrick, *Reality Check: How is the EU Ensuring Data Protection in XR Technologies?*, The Digital Constitutionalist (Jan. 25, 2023), https://digi-con.org/reality-check-how-is-the-eu-ensuring-data-protection-in-xr-technologies/.

120 For more, *see* "Stage 4: Implementing Relevant Best Practices."

121 As previously noted, this framework uses these terms "fair," "ethical," and "responsibly," broadly, and not in a legal sense.

122 *Expectations: OPC's Guide to the Privacy Impact Assessment Process*, Office of the Privacy Commissioner of Canada (Mar. 2020), https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/.

Guidelines on Data Protection Impact Assessment, European Commission (Oct. 13, 2017), https://ec.europa.eu/newsroom/article29/items/611236.

123 GDPR requires personal data to be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')." Regulation (EU) 2016/679 Art. 5(1)(c), https://gdpr-info.eu/art-5-gdpr/.

Minimization under the Fair Information Practice Principles require federal agencies to "only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose." *Fair Information Practice Principles*, Federal Privacy Council, https://www.fpc.gov/resources/fipps/.

Under the CCPA/CPRA, "A business'[] collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes." Cal. Civ. Code § 1798.100(c), https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

124 As with AI, organizations need "to reconcile the need for sensitive data with the principle of minimization." Andrew Burt and Brenda Leong, *AI vs. Privacy: How to Reconcile the Need for Sensitive Data with the Principle of Minimization*, IAPP (Aug. 16, 2023), https://iapp.org/news/a/ai-vs-privacy-how-to-reconcile-the-need-for-sensitive-data-with-the-principle-of-minimization/.

125 Privacy by design (PbD) can help organizations bake privacy into their products, services, and processes from the beginning. PbD includes having default settings that prioritize privacy, such as opt-in rather than opt-out; occasionally deleting identifiable data; and minimizing the identifiability, observability, and linkability of personal data. Privacy by design should be implemented throughout the organization, and data minimization should be a shared responsibility across teams. Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles*, Information & Privacy Commission: Ontario, Canada (Mar. 2011), https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf.

Ann Cavoukian, *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices*, Information & Privacy Commission: Ontario, Canada (Dec. 2012), https://www.schwaab.ch/wp-content/uploads/2013/09/operationalizing-pbd-guide.pdf.

126 Kobbi Nissim, Thomas Steinke, et al., *Differential Privacy: A Primer for a Non-Technical Audience*, Harvard University: Privacy Tools for Sharing Research Data (Mar. 3, 2017), https://privacytools.seas.harvard.edu/files/privacytools/files/pedagogical-document-dp_0.pdf.

When organizations need sensitive data for purposes like bias auditing—uses which have a low risk of harm, and are intended to reduce discrimination—organizations can use intentional proxies for sensitive data based on data they already have, to minimize further collection. For example, Bayesian Improved Surname Geocoding uses zip code and surname to infer sensitive categories like gender and race/ethnicity. Andrew Burt and Brenda Leong, *AI vs. Privacy: How to Reconcile the Need for Sensitive Data with the Principle of Minimization*, IAPP (Aug. 16, 2023), https://iapp.org/news/a/ai-vs-privacy-how-to-reconcile-the-need-for-sensitive-data-with-the-principle-of-minimization/.

Miranda Bogen, Pushkar Tripathi, et al., *Towards Fairness in Personalized Ads*, Meta (Jan. 2023), https://about.fb.com/wp-content/uploads/2023/01/Toward_fairness_in_personalized_ads.pdf.

127 Yuanjie Wu, Yu Wang, et al., *Using a Fully Expressive Avatar to Collaborate in Virtual Reality: Evaluation of Task Performance, Presence, and Attraction*, Frontiers in Virtual Reality (Apr. 7, 2021), https://www.frontiersin.org/articles/10.3389/frvir.2021.641296/full.

128 *See* "Stage 3: Identifying and Assessing Risks to Individuals, Communities, and Society."

129 "As an example of how data minimization might work in practice, suppose a wearable device, such as a patch, can assess a consumer's skin condition. The device does not need to collect precise geolocation information in order to work; however, the device manufacturer believes that such information might be useful for a future product feature that would enable users to find treatment options in their area. As part of a data minimization exercise, the company should consider whether it should wait to collect geolocation until after it begins to offer the new product feature, at which time it could disclose the new collection and seek Consent." *Internet of Things - Privacy & Security in a Connected World*, FTC (Nov. 2013), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

130 Regulatory sandboxes shield organizations from legal risk. In its "metaverse" strategy, the EU is proposing a regulatory sandbox. Jack Schickler, *EU's Leaked Metaverse Strategy Proposes Regulatory Sandbox, New Global Governance*, CoinDesk (July 6, 2023), https://www.coindesk.com/policy/2023/07/06/eus-leaked-metaverse-strategy-proposes-regulatory-sandbox-new-global-governance/.

131 For more on developing a data retention policy, *see* Jeremiah S. Wikler, *Document Retention Policy Checklist*, Reuters (April 3, 2023), https://www.reuters.com/practical-law-the-journal/litigation/document-retention-policy-checklist-2023-04-03/.

132 GDPR Art. 5(1)(b) states that "[p]ersonal data shall be … collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes." Regulation (EU) 2016/679 Art. 5(1)(b), https://gdpr-info.eu/art-5-gdpr/.

The CCPA/CPRA states that "[a] business shall not collect additional categories of personal information or use personal information collected for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected, without providing the consumer with notice consistent with this section." Cal. Civ. Code § 1798.100(a)(1), https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

133 For example, using body motion data to predict an individual's "criminality" has a high likelihood of resulting in discrimination and/or harm. Julia Dressel and Hany Farid, *The Dangers of Risk Prediction in the Criminal Justice System*, MIT Case Studies in Social and Ethical Responsibilities of Computing (Feb. 5, 2021), https://mit-serc.pubpub.org/pub/risk-prediction-in-cj/release/2.

134 Brooke Auxier, Lee Rainie, et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

135 *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FTC (May 2021), https://www.ftc.gov/about-ftc/mission/enforcement-authority.

136 *Internet of Things - Privacy & Security in a Connected World*, FTC Staff Report (Nov. 2013), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

137 *Progressive Disclosure*, Interaction Design Foundation, https://www.interaction-design.org/literature/topics/progressive-disclosure.

138 New interfaces, such as those found in immersive technologies, also open the door for novel design practices that deceive or manipulate users into providing consent or disclosing more data. Organizations should avoid these practices, which resemble "dark patterns." *Bringing Dark Patterns to Light*, FTC Report (Sept. 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.

139 "Ambient notifications" use elements within an application's design to guide users' attention to the notification in a way that is less likely to disrupt the experience. For more on how VR designers are thinking about incorporating device notifications (rather than privacy disclosures) in an unobtrusive way, *see* André Zenner, Marco Speicher, et al., *Immersive Notification Framework: Adaptive & Plausible Notifications in Virtual Reality*, CHI'18 Extended Abstracts (Apr. 2018), https://www.dfki.de/fileadmin/user_upload/import/9735_CHI2018-LBW-Immersive-Notification.pdf.

140 For ideas about how designers are currently working through this, *see Data Transparency and Control in XR and the Metaverse: Early UX Explorations with People in APAC*, Meta Report (June 2023), https://www.ttclabs.net/site/assets/files/11085/data_transparency_and_control_in_xr_and_the_metaverse_report.pdf.

141 *The State of Play: Verifiable Parental Consent and COPPA,* Future of Privacy Forum (June 2023), https://fpf.org/verifiable-parental-consent-the-state-of-play/.

Felicity Slater, *The Future of Manipulative Design Regulation*, Future of Privacy Forum Blog (Jan. 19, 2023), https://fpf.org/blog/the-future-of-manipulative-design-regulation/.

142 *See U.S. v. Microsoft Corporation*, Case No. 2:23-CV-836 (W.D. Wash filed June 5, 2023) (holding that "the direct notice failed to describe Defendant's collection and use practices with regard to personal information collected from children and instead directed parents to the company's online notice of its information practices.") While this case specifically discussed notice in the context of children and COPPA, contextual notice is recommended for all users. https://www.ftc.gov/system/files/ftc_gov/pdf/microsoftcomplaintcivilpenalties.pdf.

143 *Data Transparency and Control in XR and the Metaverse*, Meta Trust, Transparency & Control Labs (June 2023), https://www.ttclabs.net/site/assets/files/11085/data_transparency_and_control_in_xr_and_the_metaverse_report.pdf.

144 Kyle Orland, *Meta Establishes 4-Foot "Personal Boundary" to Deter VR Groping*, Ars Technica (Feb. 7, 2022), https://arstechnica.com/gaming/2022/02/meta-establishes-four-foot-personal-boundary-to-deter-vr-groping/.

Block or Unblock Someone in Meta Horizon Worlds, Meta (last updated July 2023), https://www.meta.com/help/quest/articles/horizon/safety-and-privacy-in-horizon-worlds/block-or-unblock-horizon/.

145 Ryan Calo, *Against Notice Skepticism In Privacy (And Elsewhere)*, Notre Dame Law Review (Mar. 2011), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1790144.

146 Evan Selinger, Ely Altman, et al., *Eye-Tracking in Virtual Reality*, Privacy Studies Journal (Mar. 24, 2023), https://tidsskrift.dk/privacy_studies_journal/article/view/134656.

147 *What Methods Can We Use to Provide Privacy Information?*, Information Commissioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/.

148 *Mobility Data Sharing Assessment: Operator's Manual*, Future of Privacy Forum and SAE Industry Technologies Consortia (Aug. 2021), https://fpf.org/wp-content/uploads/2021/08/2-MDSA-Operators-Manual.pdf.

149 *What Methods Can We Use to Provide Privacy Information?*, Information Commissioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/.

150 *Id*.

151 Patrick Gage Kelley, Joanna Bresee, et al., *A "Nutrition Label" for Privacy*, Symposium on Usable Privacy and Security (July 2009), https://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf.

152 Evan Selinger, Ely Altman, et al., *Eye-Tracking in Virtual Reality*, Privacy Studies Journal (Mar. 24, 2023), https://tidsskrift.dk/privacy_studies_journal/article/view/134656.

153 Joseph Jerome and Jeremy Greenberg, *Augmented Reality + Virtual Reality: Privacy and Autonomy Considerations in Emerging, Immersive Digital Worlds*, Future of Privacy Forum (Apr. 2021), https://fpf.org/wp-content/uploads/2021/04/FPF-ARVR-Report-4.16.21-Digital.pdf.

154 *Introducing the New Ray-Ban | Meta Smart Glasses*, Meta Newsroom (Mar. 27, 2023), https://about.fb.com/news/2023/09/new-ray-ban-meta-smart-glasses/.

155 *See* Joseph O'Hagan, Pejman Saeghe, et al., *Privacy-Enhancing Technology and Everyday Augmented Reality: Understanding Bystanders' Varying Needs for Awareness and Consent*, Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (Dec. 5, 2022), https://eprints.gla.ac.uk/282546/1/282546.pdf.

Matthew Corbett, Brendan David-John, et al., *BystandAR: Protecting Bystander Visual Data in Augmented Reality Systems*, MobiSys 2023: Proceedings of the 21st Annual International Conference on Mobile Systems, Applications and Services (June 2023), https://dl.acm.org/doi/abs/10.1145/3581791.3596830.

156 Automatically blurring faces may raise legal questions regarding whether collecting face data of bystanders for the purpose of blurring their faces—which requires an initial collection and processing to blur—would violate BIPA's notice and consent requirement for biometric data. If interpreted in such a way, it would discourage organizations from engaging in this privacy-enhancing practice. Jim Nash, *Blurring a Face on YouTube Can Violate BIPA – New Lawsuit*, Biometric Update (Sept. 2, 2022), https://www.biometricupdate.com/202209/blurring-a-face-on-youtube-can-violate-bipa-new-lawsuit.

157 *E.g.*, The CCPA/CPRA grants consumers rights to access, correction, and deletion, among other rights. Cal. Civ. Code §§ 1798.105 *et seq*., https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

158 "In terms of user experience (UX) and content strategy, many of the paradigms we held in the age of 2D mobile applications may need to be expanded and adapted for 3D interactions. We are now on the journey of reimagining how humans interact with computers as something much more fluid and immersive." *Data Transparency and Control in XR and the Metaverse: Early UX explorations with people in APAC*, Meta Report (Jun. 2023), https://www.ttclabs.net/site/assets/files/11085/data_transparency_and_control_in_xr_and_the_metaverse_report.pdf.

159 Pete Swabey, *Why Edge Computing is a Double-Edged Sword for Privacy*, Tech Monitor (Feb. 23, 2022), https://techmonitor.ai/focus/privacy-on-the-edge-why-edge-computing-is-a-double-edged-sword-for-privacy.

160 Joseph Jerome, *Where You Look Is Personal*, Tech Policy Press (June 6, 2023), https://techpolicy.press/where-you-look-is-personal/.

161 *Biometric Recognition and Authentication Systems*, U.K. National Cyber Security Centre, https://www.ncsc.gov.uk/collection/biometrics/general-principles.

162 Jon Radoff, *The Metaverse Value-Chain*, Medium (Apr. 7, 2021), https://medium.com/building-the-metaverse/the-metaverse-value-chain-afcf9e09e3a7.

163 "If you signed a SDLA [software development licensing agreement] for commercial use and have been granted [the] right to store and or transfer eye tracking or attention computing data, you also have to undergo a review process (this is not applicable for applications under the Research SDLA)." *Data Transparency Policy*, Tobii, https://www.tobii.com/company/tobii-eye-tracking-data-transparency-policy.

164 Researchers conduct data flow analyses to study application data leakage, and organizations could integrate it into their due diligence process. Benjamin Andow, Samin Yaseer Mahmud, et al., *Actions Speak Louder than Words: Entity-Sensitive Privacy Policy and Data Flow Analysis with POLICHECK*, 29th USENIX Security Symposium (Aug. 2020), https://www.usenix.org/system/files/sec20summer_andow_prepub.pdf.

Jingjing Ren, Ashwin Rao, et al., *ReCon: Revealing and Controlling PII Leaks in Mobile Network Traffic*, arXiv (July 1, 2015), https://arxiv.org/abs/1507.00255.

165 "Tobii customers and partners that are developing solutions requiring access to our API's, need to sign a software development license agreement (SDLA). Our SDLA for commercial use and for research use requires compliance to the Tobii data transparency policy." *Data Transparency Policy*, Tobii, https://www.tobii.com/company/tobii-eye-tracking-data-transparency-policy.

166 Tobii's transparency policy, in regards to hardware manufacturers and OEMs, states: "If you wish to publish your own proprietary SDKs or APIs that incorporate our technology, you must contact us to ensure that our data transparency policy is upheld." *Data Transparency Policy*, Tobii, https://www.tobii.com/company/tobii-eye-tracking-data-transparency-policy.

167 Helen Nissenbaum, *Symposium: Privacy as Contextual Integrity*, Washington Law Review (2004), https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/.

168 Sara Jordan, Elizabeth Arledge, et al., *The Playbook: Data Sharing for Research*, Future of Privacy Forum (Dec. 2022), https://fpf.org/wp-content/uploads/2022/12/FPF-Playbook-singles.pdf.

Allowing researchers to access organizational data can also benefit the organization sharing the data, as it can lead to improvements in their products and services. Shea Swauger and Marjory S. Blumenthal, *Report: Data Sharing for Research - A Compendium of Case Studies, Analysis, and Recommendations*, Future of Privacy Forum (Aug. 2022), https://fpf.org/wp-content/uploads/2023/08/FPF-Data-Sharing-for-Research-Compendium-R5-Digital-1.pdf.

169 Birtukan Birawo and Pawel Kasprowski, *Review and Evaluation of Eye Movement Event Detection Algorithms*, Sensors Journal (Nov. 15, 2022), https://www.mdpi.com/1424-8220/22/22/8810.

170 For example, if a third party only needs a user's eye "fixations"—where their gaze focuses—but not "saccades"—rapid movements between fixation points—organizations should refrain from disclosing the latter. Saccades can be used to infer health conditions, and so could be high-risk. Pichet Termsarasab, Thananan Thammongkolchai, et al., *The Diagnostic Value of Saccades in Movement Disorder Patients: A Practical Guide and Review*, Journal of Clinical Movement Disorders (Oct. 15, 2015), https://clinicalmovementdisorders.biomedcentral.com/articles/10.1186/s40734-015-0025-4.

171 Florian Wiedmann, *What is a Trusted Execution Environment (TEE) and How Can it Improve the Safety of Your Data?*, Piwik (July 1, 2021), https://piwik.pro/blog/what-is-a-trusted-execution-environment/.

Chuan Chen, Yuecheng Li, et al., *Privacy Computing Meets Metaverse: Necessity, Taxonomy and Challenges*, IEEE Internet of Things Journal (Oct. 17, 2023), https://arxiv.org/pdf/2304.11643.pdf.

172 Daniel Goldberg and Rick Borden, *Regulators and Litigators are Investigating Data Flows Through SDKs – An Overview and Practical Steps to Reduce Risk*, Frankfurt Kurnit Klein & Selz (Aug. 23, 2023), https://technologylaw.fkks.com/post/102imku/regulators-and-litigators-are-investigating-data-flows-through-sdks-an-overview.

For example, Apple Vision Pro's SDK sets strict terms and conditions for third party developers building on the platform. Emma Roth, *Apple is Taking Applications for Vision Pro Developer Kits*, The Verge (Jul. 24, 2023), https://www.theverge.com/2023/7/24/23805883/apple-vision-pro-ar-headset-developer-kit.

173 Michael Garcia, *The Forgotten "Emerging" Technology: The Metaverse and Its Cybersecurity Implications*, New America (Sept. 25, 2023), https://www.newamerica.org/future-security/reports/the-forgotten-emerging-technology/.

174 *Data Breach Response: A Guide for Business*, FTC (Feb. 2021), https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business.

175 Jules Polonetsky and Jeremy Greenberg, *NSF Convergence Accelerator: The Future of Privacy Technology (C-Accel 1939288)*, Future of Privacy Forum (Mar. 2020), https://fpf.org/wp-content/uploads/2020/03/NSF_FPF-REPORT_C-Accel1939288_Public.pdf.

176 Peter Loshin, *Definition: Encryption*, TechTarget (last updated June 2022), https://www.techtarget.com/searchsecurity/definition/encryption.

177 Kobbi Nissim, Thomas Steinke, et al., *Differential Privacy: A Primer for a Non-Technical Audience*, Harvard University: Privacy Tools for Sharing Research Data (Mar. 3, 2017), https://privacytools.seas.harvard.edu/files/privacytools/files/pedagogical-document-dp_0.pdf.

178 *How Should We Assess Security and Data Minimisation in AI?*, Information Commissioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-should-we-assess-security-and-data-minimisation-in-ai/.

179 *What Is Multiparty Computation?*, IEEE Digital Privacy, https://digitalprivacy.ieee.org/publications/topics/what-is-multiparty-computation.

180 *How Should We Assess Security and Data Minimisation in AI?*, Information Commissioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-should-we-assess-security-and-data-minimisation-in-ai/.

181 For more on implementing PETs within organizations *see* Maria Badillo, *Navigating Privacy-Enhancing Technologies: Key Takeaways from the Inaugural Meeting of the Global PETs Network*, Future of Privacy Forum (Sept. 7, 2023), https://fpf.org/blog/navigating-privacy-enhancing-technologies-key-takeaways-from-the-inaugural-meeting-of-the-global-pets-network/.

182 Bailey Sanchez and Jim Siegl, *New FPF Infographic Analyzes Age Assurance Technology & Privacy Tradeoffs*, Future of Privacy Forum (June 26, 2023), https://fpf.org/blog/new-fpf-infographic-analyzes-age-assurance-technology-privacy-tradeoffs/.

183 Andrew Burt and Brenda Leong, *AI vs. Privacy: How to Reconcile the Need for Sensitive Data with the Principle of Minimization*, IAPP (Aug. 16, 2023), https://iapp.org/news/a/ai-vs-privacy-how-to-reconcile-the-need-for-sensitive-data-with-the-principle-of-minimization/.

184 Jack Schickler, *EU's Leaked Metaverse Strategy Proposes Regulatory Sandbox, New Global Governance*, CoinDesk (July 6, 2023), https://www.coindesk.com/policy/2023/07/06/eus-leaked-metaverse-strategy-proposes-regulatory-sandbox-new-global-governance/.

185 Cal. Civ. Code §§ 1798.100 to 1798.199.100, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

186 Colo. Rev. Stat. §§ 6-1-1301 to 6-1-1313, https://law.justia.com/codes/colorado/2022/title-6/article-1/part-13/.

187 Conn. Gen. Stat. §§ 42-515 to 42-525, https://law.justia.com/codes/connecticut/2022/title-42/chapter-743jj/section-42-515/.

188 84 Del. Laws §§ 12D-101 to 12D-111, https://delcode.delaware.gov/title6/c012d/index.html.

189 Fla. Stat. §§ 501.701 to 501.722, http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0500-0599/0501/0501PartVContentsIndex.html&StatuteYear=2023&Title=%2D%3E2023%2D%3EChapter%20501%2D%3EPart%20V.

190 Ind. Code §§ 24-15-1-1 to 24-15-11-2, https://iga.in.gov/laws/2023/ic/titles/24#24-15.

191 Iowa Code §§ 715D.1 to 715D.9, https://casetext.com/statute/code-of-iowa/title-xvi-criminal-law-and-procedure/chapter-715d.

192 Mont. Code Ann. §§ 30-14-2801 to 30-14-2817, https://leg.mt.gov/bills/mca/title_0300/chapter_0140/part_0280/sections_index.html.

193 Or. S.B. 619 (2023), https://olis.oregonlegislature.gov/liz/2023R1/Downloads/MeasureDocument/SB619/Enrolled.

194 Tenn. H.B. 1181 (2023), https://publications.tnsosfiles.com/acts/113/pub/pc0408.pdf.

195 Tex. Bus. & Com. Code §§ 541.001 to 541.205, https://statutes.capitol.texas.gov/Docs/BC/htm/BC.541.htm.

196 Utah Code Ann. §§ 13-61-101 to 13-61-404, https://le.utah.gov/xcode/Title13/Chapter61/13-61.html.

197 Va. Code Ann. §§ 59.1-575 to 59.1-584, https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/.

198 740 Ill. Comp. Stat. Ann. §§ 14/1 to 14/25, https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

199 Tex. Bus. & Com. Code § 503.001, https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm.

200 Wash. Rev. Code §§ 19.375.010 to 19.375.900, https://app.leg.wa.gov/RCW/default.aspx?cite=19.375&full=true.

201 *E.g.*, Me. Rev. Stat. tit. 25 § 6001(2)(A), https://legislature.maine.gov/statutes/25/title25sec6001.html; Fla. Stat. Ann. § 1002.222, http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=1000-1099/1002/1002.html; Idaho Code § 33-133, https://legislature.idaho.gov/statutesrules/idstat/Title33/T33CH1/SECT33-133/; Kan. Stat. Ann. § 72.6315, http://ksrevisor.org/statutes/chapters/ch72/072_063_0015.html; Mo. Rev. Stat. § 161.096(3), https://revisor.mo.gov//main/OneSection.aspx?section=161.096&bid=7851&hl=; Colo. Rev. Stat. § 2-3-1701, https://casetext.com/statute/colorado-revised-statutes/title-2-legislative/legislative-services/article-3-legislative-services/part-17-joint-technology-committee/section-2-3-1707-task-force-for-the-consideration-of-facial-recognition-services-creation-membership-duties-compensation-staff-support-repeal.

202 15 U.S.C. §§ 6501 to 6505, https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312.

203 *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FTC (May 2021), https://www.ftc.gov/about-ftc/mission/enforcement-authority.

For more on the FTC's perspective on AI, *see* Michael Atleson, *The Luring Test: AI and the Engineering of Consumer Trust*, FTC (May 1, 2023), https://www.ftc.gov/business-guidance/blog/2023/05/luring-test-ai-engineering-consumer-trust.

Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act, FTC (May 18, 2023), https://www.ftc.gov/legal-library/browse/policy-statement-federal-trade-commission-biometric-information-section-5-federal-trade-commission.

204 45 CFR Part 160, Part 162, and Part 164, https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C.

205 Wash. Rev. Code §§ 19.373.005 - 19.373.900, https://app.leg.wa.gov/RCW/default.aspx?cite=19.373.

206 Nev. S.B. 370, https://www.leg.state.nv.us/App/NELIS/REL/82nd2023/Bill/10323/Text.

FUTURE OF PRIVACY FORUM

1350 EYE STREET NW | SUITE 350 | WASHINGTON, DC 20005 FPF.ORG | info@fpf.org