VOLUME 4 April 2023 ISSUE 1

JOURNAL ON EMERGING TECHNOLOGIES

ARTICLES

EXTENDED PRIVACY FOR EXTENDED REALITY: XR TECHNOLOGY HAS 99 PROBLEMS AND PRIVACY IS SEVERAL OF THEM

Suchismita Pahi & Calli Schroeder

Americans are rapidly adopting innovative technologies which are pushing the frontiers of reality. But, when they look at how their privacy is protected within the new extended reality (XR), they will find that U.S. privacy laws fall short. The privacy risks inherent in XR are inadequately addressed by current U.S. data privacy laws or court-created frameworks that purport to protect the constitutional right to be free from unreasonable searches. Many scholars, including Ryan Calo, Danielle Citron, Sherry Colb, Margaret Hu, Orin Kerr, Kirsten Martin, Paul Ohm, Daniel Solove, Rebecca Wexler, Shoshana Zuboff, and others, have highlighted the gaps in U.S. privacy protections stemming from big data, artificial intelligence, and increased surveillance technologies.

However, the depth and breadth of what XR technology reveals about a person, the risks it poses to bystanders, and the imminent paradigm shift of a public space versus a private space are new problems. This paper provides three central contributions for technologists, legislators, and anyone interested in privacy rights: first, a brief guide to understanding XR technology; second, a survey of the current U.S. privacy landscape and the gaps in U.S. privacy protections for XR; and third, an easily digestible list of solutions that legislators and technologists can pursue to better protect privacy in XR.

EXTENDED PRIVACY FOR EXTENDED REALITY: XR TECHNOLOGY HAS 99 PROBLEMS AND PRIVACY IS SEVERAL OF THEM

Suchismita Pahi & Calli Schroeder[*]

"*I forgot I was in virtual reality and I got grounded, and now I'm grounded in real life.*"

- Leopold "Butters" Stotch[1]

INTRODUCTION

Augmented Reality, Virtual Reality, and Mixed Reality (collectively, "extended reality" or "XR") are poised to explode in use in the United States ("U.S.").[2] XR technologies present unique risks to privacy by enmeshing the real world with the imagined. XR technologies exacerbate existing privacy concerns related to artificial intelligence and big data and introduce new privacy risks for bystanders. On top of these risks, existing privacy regulations that address virtual or real-world privacy issues fail to adequately address the convergence of realities that exists in XR. These privacy risks heighten the urgency of developing substantive protections for both users and bystanders from privacy intrusions previously only imagined in cyber dystopian fiction.[3]

XR technologies typically involve one or more wearable devices that include cameras, microphones, and sensors that collect a vast array

[*] This paper is the result of 2 years of virtual collaboration during the chaos of the pandemic(s). We would like to express our deep gratitude to fellow practitioners who have taken the time to read and comment, or otherwise provide thoughtful feedback, challenge assumptions, and provide assessments and encouragement throughout this endeavor: Alyssa Feola, Madaleine Gray, Mike Hintze, Joel Scharlat, Ben Steinberger, and our families for their support, with apologies to anyone whom we might have omitted. The views in this paper do not reflect the views of either of our employers: Databricks, Inc. or the Electronic Privacy Information Center (EPIC).

[1] *South Park: Grounded Vindaloop* (Comedy Central broadcast Nov.12, 2014).

[2] 4 PERKINS COIE LLC ET AL., 2020 AUGMENTED AND VIRTUAL REALITY SURVEY REPORT (2020), https://www.perkinscoie.com/images/content/2/3/v4/231654/2020-AR-VR-Survey-v3.pdf; Magic Leap, *Demos: Waking Up with Mixed Reality,* YOUTUBE (Apr. 19, 2016), https://youtu.be/GmdXJy_IdNw (an example of "Mixed Reality").

[3] *See, e.g.,* MASAMUNE SHIROW, GHOST IN THE SHELL (1st ed. 1989); LAUREN BEUKES, MOXYLAND (2008); PHILIP K. DICK, UBIK (1969); Ray Bradbury, *The World the Children Made*, SATURDAY EVENING POST (Sept. 23, 1950).

of information about the user and their environment.[4] And XR data collection and use does not stop at external data or solely physical data or even inferences from that data. XR technology also includes neural activity tech, such as brain-computer interfaces (BCI), that companies are developing to make the XR experience less clumsy and more intuitive.[5] As the technology advances, these devices will inevitably become more ubiquitous. They can collect information about not just the user, but also bystanders—which could be children, strangers, intimate partners, or anyone else. And their portability means that they collect information not just within the intimacy of the user's own home (which itself raises a several potential privacy and safety concerns) but also a wide range of public and private places—including hospitals, shelters, restrooms, places of worship, and more.

Current U.S. privacy regulation has failed to evolve with technology, leaving Americans at the mercy of a personal privacy trade-off that is often made without the individual's full knowledge. XR technologies are making inroads into businesses, healthcare,[6] schools, marketing, and leisure, generating millions of data points that can be used to extrapolate, infer, and create profiles on users and bystanders alike—and may subsequently be used to manipulate, target, provide, and deny services with limited or no meaningful choices or options for those users and bystanders.[7] This paper enumerates the privacy risks present in and unique to XR and the regulatory gaps in privacy protections from this technology. Please note that the terms "XR," "XR technology," and "XR technologies" may all be used within the paper and collectively refer to the devices and systems used to create and support extended reality.

Potential privacy risks from XR include legal and real-world harms ranging from expanded surveillance and data collection methods for law enforcement and intelligence agencies to long-term harms

---

[4] Keiichi Matsuda, *Hyper-Reality,* YOUTUBE (May 19, 2016), https://youtu.be/YJg02ivYzSs (Keiichi Matsuda, former director of Microsoft and current director of LiquidCity, created a video that demos what to many is the worst case scenario of XR).

[5] *See, e.g.*, OpenBCI, https://openbci.com/ (last visited Nov. 9, 2022) (the open source efforts by OpenSourceBCI to assist in enabling biosensing).

[6] *See, e.g.,* DEEPVR, https://www.exploredeep.com/#about-deep (last visited Nov. 9, 2022) (Deep VR, a meditative reality game developed to interface with head mounted gear and purporting to reduce user anxiety).

[7] Frank Pasquale, *7 Ways Data Currently Being Collected About You Could Hurt Your Career or Personal Life,* HUFFPOST (Nov. 6, 2014, updated Dec. 6, 2017), https://www.huffpost.com/entry/data-collected-hurt-career-personal_b_6110682; Will Knight, *Job Screening Service Halts Facial Analysis of Applicants,* WIRED (Jan. 12, 2021), https://www.wired.com/story/job-screening-service-halts-facial-analysis-applicants/.

stemming from corporate black box decision-making for users, bystanders, and households.[8] Our analysis explores the limits of existing U.S. privacy doctrines and of Fourth Amendment protections against unreasonable searches. Current U.S. privacy regulation largely fails to recognize privacy harms for individuals when grounded in loss of data or impacts from data without a direct tie to a financial, physical, or otherwise calculable loss or a historically recognized harm, such as intrusion or unlawful disclosure.[9] This failure is magnified in the big data analytics context and proves particularly insufficient to meaningfully protect individuals in the XR context.[10]

Various technologists recognize that there are privacy problems with big data, including big data processed in XR, and attempt to mitigate these privacy problems through technical measures.[11] However, these attempts are not a substitute for substantive legal privacy protections that fully address XR technologies themselves. Existing regulations are likely to exclude XR due to narrowly tailored scope meant to address a

---

[8] *See* United States v. Jones, 565 U.S. 400 (2012); Kyllo v. United States, 533 U.S. 27 (2001); Carpenter v. United States, 138 S. Ct. 2206 (2018); FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (Harvard Univ. Press, 2015).

[9] *See* Jackson v. Abendroth & Russell, P.C., 207 F. Supp. 3d 945 (S.D. Iowa 2016); Mey v. Got Warranty, Inc., 193 F. Supp. 3d 641 (N.D.W. Va. 2016); Laurie Segall, *Pastor Outed on Ashley Madison Commits Suicide*, CNN MONEY (Sept. 8, 2015, 7:10 PM), http://money.cnn.com/2015/09/08/technology/ashley-madison-suicide (Ashley Madison's parent company, Avid Life Media, acknowledged the connection between an affected user's suicide and the privacy violation in its statement "Dr. Gibson's passing is a stark, heart-wrenching reminder that the criminal hack against our company and our customers has had very real consequences for a great many innocent people."); Letter from Senator Ron Wyden to Avril D. Haines, Director, Nat'l Intel. (Apr. 13, 2021) (on file with author) https://www.wyden.senate.gov/imo/media/doc/HainesBurns_WydenHeinrich_13APR21%20-FINAL.pdf.

[10] Big data is not defined uniformly in the tech industry. However, it can generally be understood to mean large volume, high velocity, and variety of data. This means a big data set is going to have a high volume of data that is increasing exponentially and is also large in scope (data types). The data may be structured, unstructured, or both. *See* Univ. Wis., *What is Big Data* (last visited Aug. 25, 2022), https://datasciencedegree.wisconsin.edu/data-science/what-is-big-data/.

[11] Zhi Xu & Sencun Zhu, *SemaDroid: A Privacy-Aware Sensor Management Framework for Smartphones*, 2015 CODASPY '15: PROC. 5TH ACM CONF. ON DATA & APP. SEC. & PRIV. 61 (2015) (proposing method to restrict sensor data access and sharing on smartphones); Franziska Roesner, et. al., *World-Driven Access Control for Continuous Sensing*, 2014 CCS '14: PROC. 2014 ACM SIGSAC CONF. ON COMPUT. & COMM'NS SEC. https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/wdac-tr.pdf (proposing a method for automated context sensing to protect privacy and limit data collection or disclosure); Jeremy Bailenson, *Protecting Nonverbal Data Tracked in Virtual Reality*, 2018 J. MED. ASS'N PEDIATRICS 905 (raising concerns about the inferences or derivations of medical diagnoses from non-verbal data points gathered by virtual reality technologies).

different technology space. For example, the types of biometrics collected in XR may not trigger regulations targeted at biometrics used specifically as identifiers in existing technologies (e.g., iPhone FaceID), even though the data itself is directly related to biological measurements (e.g. height, gait, heart rate).

In addition to the risks XR poses to user privacy, XR also creates greater and significant risks for bystander privacy. Processing of bystander data poses a crucial unaddressed privacy risk because a bystander does not have awareness that their information is being collected and does not have a way of opting out of said information collection.[12] This is especially problematic in the case of biometric data since neither users nor bystanders have the ability to change that information without surgical intervention or other highly-invasive and class-accessible actions. You can't change your faceprint.

Facebook recently revealed a partnership with Ray-Ban to create eyeglasses that can be used for XR purposes.[13] The glasses are unobtrusive and have to be linked with the user's Facebook account.[14] The only indication to bystanders of these glasses' XR capability is a small red light on the frames.[15] While the Ray-Ban capabilities are currently relatively limited, it is a foray into XR that can only grow and immediately implicates bystander privacy by allowing recordings that are not easily detectable by the bystander. These recordings are not necessarily secret, but they are also not easily detected and are unexpected by the general U.S. public. Facebook's repeated overtures into the "metaverse," including rebranding as "Meta Platforms, Inc." to demonstrate its commitment to XR, add to already existing concerns about the massive data repository that will be available to Facebook to use at will if it moves virtually unregulated into the space.[16]

---

[12] While notice and choice paradigms are common, post-user experience and user interaction design phases, the choice/consent opt-in opt-out format often leads to an overwhelming set of choices for users. This problem has been explored by others in much more detail and we will not rehash these arguments here. *See, e.g.*, Richard Warner, *Notice and Choice Must Go: The Collective Control Alternative*, 23 SMU SCI. & TECH. L. REV. 173 (2020); Claire Park, *How "Notice and Consent" Fails to Protect Our Privacy,* NEW AM. (Mar. 23, 2020), https://www.newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy/.

[13] Lucas Matney, *Review: Facebook's Ray-Ban Stories Make the Case for Smart Glasses,* TECHCRUNCH (Sept. 9, 2021, 12:02 PM), https://techcrunch.com/2021/09/09/facebooks-first-smart-glasses-make-the-case-for-face-worn-wearables.

[14] *Id.*

[15] *Id.*

[16] *Facebook Wants to Lean into the Metaverse. Here's What It Is and How It Will Work,* NPR (Oct. 28, 2021, 8:20 PM),

Setting aside legislative approaches or judicial norms, we also explore industry standards as a risk-mitigation measure. Users are unlikely to be able to rely on industry self-regulation, as industry expectations can, and often do, diverge from user expectations and may be changed with little notice to or input from users. Industries often make decisions regarding data processing activities that the public is uncomfortable with, highlighting the disconnect in public expectations and industry norms. As a real-world example, Facebook decided to collect data from and keep shadow profiles about non-users.[17] Notably, there are no state or federal regulations preventing companies from creating "shadow" profiles on behalf of users who aren't engaged with a product. Facebook, from a legal perspective, could assume creating profiles in this manner was a reasonable choice. But, from a transparency and user expectations perspective, it was evident that Facebook shot far above the target, as many non-Facebook users demonstrated discomfort with the concept of profiles created for them without any affirmative actions on their part.[18] This conflict demonstrates the misalignment between permitted uses within self-regulatory systems and individual expectations. Further, this example could easily expand in the XR space to detailed profiles being created on bystanders, including sensitive information, such as biometric information, location information, and more.

As another example of the unreliability of industry self-regulation, Facebook reassured Oculus users that they would not be required to tie their devices to a Facebook account.[19] This provided users with some assurance where they may have been interested in the gaming

---

https://www.npr.org/2021/10/28/1050280500/what-metaverse-is-and-how-it-will-work.

[17] *See, e.g.*, Russell Brandom, *Shadow Profiles Are the Biggest Flaw in Facebook's Privacy Defense,* VERGE (Apr. 11, 2018, 3:53 PM), https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy; Andrew Quodling, *Shadow Profiles - Facebook Knows About You, Even If You're Not on Facebook,* THE CONVERSATION (Apr. 13, 2018, 2:41 AM), https://theconversation.com/shadow-profiles-facebook-knows-about-you-even-if-youre-not-on-facebook-94804; Kurt Wagner, *This Is How Facebook Collects Data on You Even If You Don't Have an Account*, VOX (Apr. 20, 2018, 1:02 PM), https://www.vox.com/2018/4/20/17254312/facebook-shadow-profiles-data-collection-non-users-mark-zuckerberg.

[18] Kashmir Hill, *How Facebook Figures Out Everyone You've Ever Met,* GIZMODO (Nov. 7, 2017), https://gizmodo.com/how-facebook-figures-out-everyone-youve-ever-met-1819822691.

[19] Adi Robertson, *Facebook Is Making Oculus' Worst Feature Unavoidable*, VERGE (Aug. 19, 2020, 7:04 PM EST), https://www.theverge.com/2020/8/19/21375118/oculus-facebook-account-login-data-privacy-controversy-developers-competition.

environment but did not want to include personal information in a Facebook account for other Facebook uses. Facebook later pivoted and announced that Oculus users would now require a Facebook account to login and use new headsets, leaving users no recourse but to tie their Facebook account identities (including the identities that had been previously built by Facebook for users without a formal account) to an XR device.[20] The only other option for users was to stop using Oculus, a device which they'd purchased based on Facebook's prior representations. These examples demonstrate the potential harms of leaving XR solely to self-regulation without representation for user and bystander interests. Not only is there the risk of a disconnect between public expectation and company decisions, but individuals are often left with few options to mitigate or control any exposure or damage to themselves and their personal information. Increasing forays into XR carry correspondingly increasing privacy risks and must be addressed with privacy protections before becoming irrevocably ingrained in our society.

Current privacy protections in the U.S. have proven unable to adapt to changing privacy risks, including those raised by XR.[21] Similarly, in the context of the Fourth Amendment, existing legal protections from government intrusion are stretched thin in their applications to new technologies.[22] Between the U.S. Supreme Court's discomfort with the third party doctrine, which removes privacy protections surrounding information provided to a third party, and its decision in *Carpenter*, it appears that the judiciary is catching on to the threats that newer technologies pose to constitutional rights.[23] However, applying Fourth Amendment law as it stands today would still allow the government to ask for and receive a company's records of a user's interactions with XR technologies. This could include not just standard data points, but telemetry, metadata, and derived or inferential information—sleeping habits, travel patterns, social interactions, communications content with other users, emotional state, behavioral or cognitive patterns, and

---

[20] *Id.*

[21] *See* Katitza Rodriguez & Kurt Opsahl, *Augmented Reality Must Have Augmented Privacy,* ELEC. FRONTIER FOUND. (Oct. 16, 2020), https://www.eff.org/deeplinks/2020/10/augmented-reality-must-have-augmented-privacy.

[22] *See* Charles Ornstein, *Privacy Not Included: Federal Law Lags Behind New Tech*, PROPUBLICA (Nov. 17, 2015, 11:00 AM EST), https://www.propublica.org/article/privacy-not-included-federal-law-lags-behind-new-tech.

[23] United States v. Jones, 565 U.S. 400, 413 (2012) (Sotomayor, J., concurring); Carpenter v. United States, 138 S. Ct. 2206 (2018).

more.[24] Any restrictions on this type of data sharing would rely on both the discretion of the third party company and whether a court chose to apply the framework in *Carpenter*, as we discuss in more depth later in this paper.

In Part I, we aim to explain XR technologies, the scale of data collection within XR, and the personal data collection and use that these systems enable. Once we have established the technology and some of the privacy risks therein, Part II supplies a summary of existing privacy regulation and case law—both in the private sector and within government—and identify privacy risks inherent in XR technologies currently unaddressed in the U.S. regulatory framework. Finally, we propose some possible approaches to bridge these privacy gaps and ensure privacy protections for both users and bystanders in XR.

I. BACKGROUND

A. What is Extended Reality?

Extended Reality (also sometimes referred to as "crossed reality" and referred to herein as "XR") is an industry term referring to a spectrum of immersive computing that enables users to cross boundaries and build real-time connections between the physical world and the virtual world.[25] XR allows users to interact with an environment that is on a sliding scale of real and virtual elements. Users see and interact with characters or objects that are not "real" or "physical" using hardware and software.[26] Though initially developed primarily for gaming, XR uses are rapidly expanding into other areas, such as enabling remote surgeries or

---

[24] *See* INFO. COMM'R'S OFF., 2.2 BIG DATA, ARTIFICIAL INTELLIGENCE, MACHINE LEARNING AND DATA PROTECTION 6–7 (2017), https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

[25] Clay Bavor, *Virtual and Augmented Realities: Asking the Right Questions and Traveling the Path Ahead*, MEDIUM (May 17, 2017), https://medium.com/@claybavor/virtual-and-augmented-realities-asking-the-right-questions-and-traveling-the-path-ahead-2428b9d13c01 (Clay Bavor (Google) suggests that the various types of extended reality are better described with terms that underscore how these systems can be layered on top of one another or layered together. His suggested terms include: "computing with presence, physical computing, perceptual computing, mixed reality, or immersive reality."); *see also Extended Reality (XR)*, XR SAFETY INITIATIVE, https://xrsi.org/definition/extended-reality-xr (last visited Nov. 9, 2022) (Defined therein as "a fusion of all the realities—including Augmented Reality (AR), Virtual Reality (VR), and Mixed Reality (MR)—which consists of technology-mediated experiences enabled via a wide spectrum of hardware and software, including sensory interfaces, applications, and infrastructures.").

[26] *See also Extended Reality (XR), supra* note 25.

creating interactive virtual classrooms.[27] Experts predict that consumer spending on XR will rise from $5 billion spent in 2018 to $40 billion in 2023 while industry spending outstrips it, surging from $4 billion to $121 billion in that period.[28]

Perhaps most critically, XR is enabled by millions of different data points that, among other uses and purposes, identify the user and incorporate them into the XR world.[29] These data points include physical body movements and patterns (hands, eyes, head, gait, full body tracking), feedback from the environment and surroundings (sound, visuals, location), biometrics (blood pressure, pulse oximetry, respiration, voice prints, face prints), and responses to haptics.[30] Many of these data points, including physical body movements and patterns, biometrics, individual haptic responses, and more, will also be considered personal data, as they link to an individual.

1. Types of XR

XR is generally used as an umbrella term, referring collectively to three types of digital and physical reality combinations: Mixed Reality ("MR"), Augmented Reality ("AR"), and Virtual Reality ("VR").[31] At the leftmost point of the reality spectrum, you'll find the real-world environment. As you slide along the spectrum to the midpoint, Augmented Reality, you'll find Snapchat and Pokémon GO as the services exist now—overlaying characters, items, and scenery enhancements over a user's existing physical environment.[32] As you reach the rightmost

---

[27] Laurence Morvan, Francis Hintermann, & Armen Ovenessoff, *Preparing for the Risky World of Extended Reality*, MIT SLOAN MGMT. REV. (Dec. 17, 2019), https://sloanreview.mit.edu/article/preparing-for-the-risky-world-of-extended-reality/.

[28] *Id.*

[29] *See, e.g.*, Bailenson, *supra* note 11.

[30] *See, e.g.,* Jeremy Greenberg, *Seven Questions to Ask if You Have XR on Your Holiday Wish List,* FUTURE PRIV. F. (Dec. 16, 2020), https://fpf.org/blog/seven-questions-to-ask-if-you-have-xr-on-your-holiday-wish-list/; Smarter Every Day, *A Real Life Haptic Glove (Ready Player One Technology Today),* YOUTUBE (Mar. 1, 2018), https://youtu.be/OK2y4Z5IkZ0 (as an example of what haptics can look like in VR interfaces).

[31] *See, e.g.,* National Institute of Standards and Technology (NIST) Extended Reality Community of Interest (XR COI); *Extended Reality (XR)*, *supra* note 25.

[32] *See* Julia Tokareva, *The Difference Between Virtual Reality, Augmented Reality and Mixed Reality*, FORBES (Feb. 2, 2018, 5:28 PM EST), https://www.forbes.com/sites/quora/2018/02/02/the-difference-between-virtual-reality-augmented-reality-and-mixed-reality/?sh=3c89df892d07; *Demystifying the Virtual Reality Landscape*, INTEL, https://www.intel.com/content/www/us/en/tech-tips-and-tricks/virtual-reality-vs-augmented-reality.html; Bernard Marr, *The Important Difference Between Augmented Reality and Mixed Reality*, BERNARD

point, you'll find Virtual Reality, where we tip into Oculus Rift or Google Daydream and the entire physical reality is replaced by an artificial reality.[33] Finally, we have Mixed Reality. MR lies between AR and VR on this spectrum, but it is not simply a blend of AR/VR and the real-world environment.[34] It is instead an experience that blends the real-world environment with digitally created content, be it sound, sight, or touch, in such a way that the environments coexist and interact with each other.[35] Perhaps the best example of MR, as of the date of this writing, is Microsoft HoloLens 2 and Phillips' Azurion platform, in which surgeons wear a headset designed to enable them to manipulate 3D images and models and guide them during minimally invasive surgeries.[36]

2. Technical Definitions

While these are commonly understood definitions of the terms below, we do not purport that these definitions are universally accepted.[37] However, definitions are critical for policymaking, so we have provided the definitions we are generally using in this paper for clarity.[38]

MARR & CO., https://bernardmarr.com/default.asp?contentID=1912 (last visited Aug. 27, 2022).

[33] *See* Tokareva, *supra* note 32; *Demystifying the Virtual Reality Landscape*, *supra* note 32; Marr, *supra* note 32.

[34] *See* Nancy Gupton, *What's the Difference Between AR, VR, and MR?*, FRANKLIN INST. (last updated Jan. 6 2020), https://www.fi.edu/difference-between-ar-vr-and-mr; Tokareva, *supra* note 32.

[35] *See* Tokareva, *supra* note 32; *Demystifying the Virtual Reality Landscape*, *supra* note 32; Marr, *supra* note 32.

[36] *See* Michele Cohen Marill, *Hey Surgeon, Is That a HoloLens on Your Head?,* WIRED (Nov. 21, 2019, 7:00 AM), https://www.wired.com/story/hey-surgeon-is-that-a-hololens-on-your-head/; *Philips and Microsoft Showcase Augmented Reality for Image-Guided Minimally Invasive Therapies,* DIAGNOSTIC & INTERVENTIONAL CARDIOLOGY (Feb. 25, 2019), https://www.dicardiology.com/content/philips-and-microsoft-showcase-augmented-reality-image-guided-minimally-invasive-therapies.

[37] Franziska Roesner et al., *Augmented Reality: Hard Problems of Law and Policy,* 2014 ACM INT'L JOINT CONF. ON PERVASIVE & UBIQUITOUS COMPUT. (UBICOMP '14): ADJUNCT PUBLICATION 1283 (2014). Other legal scholars have distilled the general properties of XR to include: sensing properties about the physical world; processing in real time; outputting information to the user, including via visual, audio, and haptic means, often overlaid on the user's perception of the physical world; providing contextual information; recognizing and tracking real-world objects; and being mobile or wearable.

[38] These definitions are taken and expanded from The XRSI Definitions of Extended Reality (XR). *See The XRSI Taxonomy of XR*, XR SAFETY INITIATIVE, https://xrsi.org/definitions.

Augmented Reality[39] typically "overlays digital or digitally-created content on top of a real-world environment," such that a user viewing the combination through a device (for example, a smartphone, AR headset, or smart glasses) will see both the digital and real-world components integrated into a real-time combination with one another to produce an enhanced and (theoretically) seamless version of reality. Both digital and virtual stimuli (e.g., graphics, sounds) may be incorporated into the AR environment in order to complete the full immersive experience. This combination allows for cohesive display, but the digital elements do not interact with the real-world environment as they do in Mixed Reality.

Mixed Reality[40] fully blends the real-world environment with digital and digitally created content, enabling the environments to coexist and interact with one another. In MR, the virtual objects are intended to commingle with and react to the real world as if they are a part of it. For example, an MR display may include digital elements that would display similar lighting patterns as if lit from the same real-world source present in the real-world environment, or sounds may echo or muffle as though they are in the same physical space as the user. As the user interacts with the combined real and virtual objects, the virtual objects should reflect the changes in the environment as would any real object in the same space.

Virtual Reality[41] is a wholly artificial digital environment. VR is composed entirely of three-dimensional virtual images experienced by users via special electronic equipment designed to display an immersive virtual environment to the user, such as a Head Mounted Display ("HMD"). The VR environment may (or may not) be modeled on real-world structures but does not actually display any physical world elements to the user—all visuals and sounds are entirely digitally generated.

B. What Kinds of Data Does XR Collect, Share, or Create?

Much of the data that XR collects, uses within its services, shares with other vendors or third parties, uses to create additional inferences,

---

[39] *Augmented Reality (AR)*, XR SAFETY INITIATIVE, https://xrsi.org/definition/augmented-reality-ar (last visited Jan. 19, 2023).
[40] *Mixed Reality (MR)*, XR SAFETY INITIATIVE, https://xrsi.org/definition/mixed-reality-mr (last visited Jan. 19, 2023).
[41] *Virtual Reality (VR)*, XR SAFETY INITIATIVE, https://xrsi.org/definition/virtual-reality-vr (last visited Jan. 19, 2023).

or otherwise processes are similar to that commonly collected by other tech services. This includes usernames, accounts, logs and records, actions taken, purchases, other users interacted with, preferences, dates of birth, age, and gender. The data may also include location data. However, XR's technical capabilities and broad reach translate into unique and heightened privacy risks to a larger cross-section of individuals.[42] These XR technologies take the existing privacy risks from virtual reality, big data analytics, and biometric data, and merge them together, adding three additional components that are particularly interesting: haptics (and related biometric responses), gathering data in near real-time, and comprehensive bystander risks.[43] While future papers may examine security concerns of XR technology, we focus specifically on the unique privacy challenges and risks in XR.

1. Personalizing Services and Profiling Users

XR collects data in a few ways, key among them being: i) from the end user with knowledge and directly; ii) from end users or bystanders indirectly and likely without knowledge or awareness; and iii) directly from third parties through contractual agreements.

End users input data directly when creating their accounts, setting up their devices, and using those devices. The data collected via this input can include name, username, age, gender, ethnicity, date of birth, sexual preference, physical identification (for example, hair, eye, or skin color), billing address, permanent residential address, financial information, search queries, preferences, and settings.

End users also—frequently without awareness or real knowledge—provide massive amounts of data points about themselves and their environments through their use of XR or XR-enabled devices. The volume of data input is often larger in scale than nearly any other form of technology thus far, particularly relating to recording and analysis of individual movement. A 2018 survey revealed that commercial XR systems typically tracked body movements 90 times per second— meaning that "spending [twenty] minutes in a VR simulation leaves just under 2 million unique recordings of body language."[44] The range of data types include location, verbal communication, physical

---

[42] *See, e.g.*, *CXOs Should Map the Risks of Extended Reality: Study*, CXO TODAY (May 17, 2019, 5:22 PM), https://www.cxotoday.com/news-analysis/cxos-should-map-the-risks-of-extended-reality-study/.
[43] *See, e.g.*, Roesner et al., *supra* note 37, at 1284.
[44] Bailenson, *supra* note 11.

movements and patterns (such as posture, gaze, gestures, physical dimensions, facial expressions, and gait), environment data (such as background, surrounding noises, or visuals), biometrics (such as blood pressure, pulse, breathing patterns, voice, or face prints), or haptic responses.[45] Several of these data types may also be collected relating to any bystanders picked up by the system sensors or the surrounding environment. These data sets may be combined with additional information from third party sources for additional inferences or other use cases. Examples of such data sets include personal details and account information from third-party systems and services (e.g., XR tech partners) or entirely separate data sets sold or shared with XR companies, such as marketing or advertising files.

The types and scale of data available from XR and third-party sources enable companies with access to the data sets to not just analyze readily viewable patterns and information, but to draw various inferences from the existing data, expanding profiles and overall information. While inferences are already drawn from existing data sets through other technical means, the inferences from XR are set apart by the sheer volume, scale, and type of data collected—particularly involuntary data—and the invasive nature of the inferences beyond those already made accessible by existing technologies. The inferences generated from XR data sets may vary widely by type.[46] They may be health or health-related inferences such as likely illness or injury from changes in activity level or motion types or ongoing physical patterns.[47] For example, researchers compared the reactions and behaviors of students diagnosed with ADHD in a VR environment with neurotypical students' reactions and behaviors to explore hypotheses about

---

[45] *Id.*; Léa Paule, *Data in the XR Industry: Why Do We Need It?*, LAVAL VIRTUAL (May 12, 2021), https://blog.laval-virtual.com/en/data-in-the-xr-industry-why-do-we-need-it/.

[46] *See* Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2019 COLUM. BUS. L. REV. 494, 506–09 (2019); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 4 (2014); VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK (2013).

[47] *See* Anthony Cuthbertson, *Google AI Can Predict When People Will Die with '95 Per Cent Accuracy'*, INDEP. (June 19, 2018, 3:32 PM), https://www.independent.co.uk/life-style/gadgets-and-tech/news/google-ai-predict-when-die-death-date-medical-brain-deepmind-a8405826.html; Alvin Rajkomar et al., *Scalable and Accurate Deep Learning with Electronic Health Records*, NPJ DIGIT. MED., May 8, 2018, at 1, 2–4; James Cook, *Amazon Patents New Alexa Feature That Knows When You're Ill and Offers You Medicine*, TEL. (Oct. 9, 2018, 6:04 PM), https://www.telegraph.co.uk/technology/2018/10/09/amazon-patents-new-alexa-feature-knows-offers-medicine/.

distractibility.[48] If researchers believe results of studies like this to be accurate in identifying particular reactions and behaviors indicative of the presence of ADHD in a user, this information could then be used to identify or diagnose ADHD through VR, potentially without the knowledge of the user.

Other inference types may include sociological inferences, such as trying to determine a user's economic status based on the type of hardware used with the XR software (possibly by combining this with their geolocation data) or based on a user's engagement in a virtual or augmented reality shopping experience.[49] XR may also be able to draw relational or networking inferences, including social groups in which an individual is active or will be active given the user's profile within XR technologies (this may include any active conditions, preferred XR software, existing ethnic, cultural, religious, or other affiliations, etc.).[50]

Existing technologies run into similar problems. For example, Tesla vehicles process location data, driver profile data, video recordings of environments while driving, and maintenance information.[51] Tesla is also planning to include haptic feedback.[52] However, unlike the Tesla, XR technologies are not limited to one industry, and can include or combine real-time processing, haptics, social interactions, audiovisual engagement, profiles, location data, and maintenance information. The convergence of this information, and the details that XR technologies can gather, is well beyond that seen in existing technologies.

---

[48] Thomas Parsons et al., *A Controlled Clinical Comparison of Attention Performance in Children with ADHD in a Virtual Reality Compared to Standard Neuropsychology Measures*, 13 CHILD NEUROPSYCHOLOGY 4, 363, 374–78 (2007).

[49] *See* José González Cabañas, Ángel Cuevas & Rubén Cuevas, Facebook Use of Sensitive Data for Advertising in Europe (Feb. 14, 2018) (unpublished manuscript) (on file with the 27th USENIX Security Symposium), https://arxiv.org/abs/1802.05030; Carter Jernigan & Behram F.T. Mistree, *Gaydar: Facebook Friendships Expose Sexual Orientation*, FIRST MONDAY (Oct. 5, 2009), https://firstmonday.org/article/view/2611/2302; Astra Taylor & Jathan Sadowski, *How Companies Turn Your Facebook Activity into a Credit Score*, NATION (May 27, 2015), https://www.thenation.com/article/archive/how-companies-turn-your-facebook-activity-credit-score/.

[50] *See* Kristen M. Altenburger & Johan Ugander, *Monophily in Social Networks Introduces Similarity Among Friends-of-Friends*, 2 NATURE HUM. BEHAV. 284, 284 (2018).

[51] Brittany Martin, *Your Tesla Is Watching – and Recording – You All the Time,* L.A. MAG. (Mar. 14, 2019), https://www.lamag.com/citythinkblog/tesla-recording-data-privacy/.

[52] Alistair Charlton, *Tesla Wants to Reinvent the Steering Wheel with Touch Control and Haptics*, GEARBRAIN (Feb. 7, 2020), https://www.gearbrain.com/tesla-patent-reinvents-steering-wheel-2645059533.html.

2. Risks of Profiling and Inferences

As we've noted above, XR has enormous potential for wide-spread use across every industry. Technologists are heralding XR as the new internet and investing heavily in it.[53] Current advertising for XR seems to focus on the gaming capabilities of the technology, but XR companies are rapidly expanding. Proposed XR uses include the health industry, the military, and practices such as explosive deactivation or conflict management, education, and workforce training (including surgical, mechanical, and emergency response training), among many other uses.[54]

The risks of XR technology must be carefully considered in light of the broad scope of potential XR use. For example, an XR device may pull data points that enable a company to conclude that a person fits into sensitive or vulnerable categories, such as transgender, labelling them as such within the system. This inference could be used for inappropriate, unethical, or offensive stereotyping by the service itself, by third parties the data is shared with, or the information could be stored in a database that is later hacked. At that point, the individual, through no affirmative action of their own, would purportedly be identified as transgender within the affected data set, now potentially available to the public. This raises questions of what XR technology could mean for individuals belonging to high-risk communities.[55]

3. Let Me Count the Ways - Privacy Risks in XR

While several of the privacy risks in XR technology are also present in other technologies, there are aspects of XR that exacerbate existing risks and, at times, create a level of privacy risk not present elsewhere. For clarity, we break the potential risks into broad categories below:

- Bystander Anonymization

---

[53] Tripp Mickle, *Apple's New Big Bet: Augmented Reality*, WALL ST. J. (June 7, 2017, 8:29 AM), https://www.wsj.com/articles/apples-new-big-bet-augmented-reality-1496779717.

[54] *See Hololens 2 x Healthcare*, MICROSOFT, https://www.microsoft.com/en-us/hololens/industry-healthcare (last visited Aug. 27, 2022) (describing Microsoft's mixed reality device and services for the healthcare industry).

[55] While this threat is not wholly unique to XR, it is still important to highlight the risk.

- Data Type and Volume
- False Data Points and Timeliness
- Misuse
- Special Categories of Persons: Children, LGBTQIA, and Other Marginalized Persons

i. Bystander Anonymization

XR technology is unlikely to solely impact the end users. It will also create almost all of the same risks for bystanders as well, although the severity of the risks may differ. For example, assume that a particular XR technology is built in such a way that it filters or blurs background sound and images, but, during the process, actually retains any verbal communications, facial geometric scanning, and precise location of a bystander(s) that were collected prior to applying the blurring effect, in its data storage. In this case, the risks to the bystander from this XR technology's database (which could result in a skeleton profile of the bystander, among other uses) are arguably at or near the same degree as to the end user of the XR technology. Privacy risks may even be higher. Bystanders have a more difficult time exercising any rights over their data as they are generally unaware that personal information has been collected, likely would not know which company or entity to contact regarding that information, and are largely left unprotected by privacy law.

It is also possible, and even probable, that technologists would prefer to incorporate technological methods to pre-emptively anonymize bystander data or enable users to do the same in the system—through blurring, selective options to enable/disable technology based on signaling, or other means, solely for the efficiency of data storage and surfacing the tech to the end user.[56] For example, engineers may introduce code that ensures certain wearable XR technology is responsive to an environment that looks like a public restroom or

[56] Jaybie A. De Guzman et al., *Security and Privacy Approaches in Mixed Reality: A Literature Survey,* ACM COMPUT. SURV., Oct. 23, 2019, at 1, 4, 13 (A survey of existing research to protect security and privacy in XR technologies.). It is probable that intrinsic input sanitization (e.g., via user-defined policies) or extrinsic input sanitization (e.g., environmental cues to anonymize or replace data) would assist in meeting the need for anonymization. This may also be true of enabling the ability to pseudo-anonymize data. However, there still remains the hazard that on some level, prior to surfacing to the user, the device or service provider is viewing identifiable information of the person. We do not have the technical knowledge to opine as to whether there are hashing, tagging, or filtering methods that may prevent identifiable information from touching the XR devices or services at all.

changing room. At that time, the wearable would cease recording or transmitting in real-time and instead delay the data flow until the wearable no longer detects the restroom environment. This would significantly reduce the privacy risks to bystanders. Again, these types of identity obfuscation or anonymization of bystander data are generally not required by the current U.S. regulatory environment, an environment which we will discuss in detail in Part II.

ii. Data Type and Volume

As mentioned earlier, a single twenty-minute session using XR technology may result in literally millions of data points collected through recordings.[57] These data points are collected for some functional purposes, such as to make the user's movements within the XR as smooth as possible and ensure that reaction time is effectively communicated within the system. However, multiple other uses of these data sets are possible. Due to the volume, consumers are unlikely to have much control or knowledge of all data points collected. For example, micromovements, frequently collected within XR technology, are largely involuntary, and individuals are not able to control them to protect or screen themselves while using the devices.[58] Tracking these micromovements could result in inferences about health conditions or injuries that the individual may not be willing to share or may be wholly unaware of. For example, in non-XR application, researchers have previously been able to use virtual classes and observe movements that indicated a higher likelihood of a particular individual having attention deficit hyperactivity disorder (ADHD) or being on the autism spectrum.[59] A company gathering these data points would then be free to use those health inferences as they choose, including targeting the individual with advertising related to, or attempting to take advantage of, the condition, or potentially sharing their inferences with third parties, such as employers.

---

[57] Bailenson, *supra* note 11 (reviewing the potential inferences about mental and behavioral health that a VR tech product could allow due to its high volume of data points on nonverbal behaviors).
[58] *Id.*
[59] *Id.*

iii. False Data Points and Timeliness

False or old data points are a significant risk of XR technology. Not only could old or inaccurate data lead to improper profiling or potential wrongful actions against the individual, but if a company makes inferences, any inferences based on or including inaccurate information will further skew data about the individual. This could result in concrete harm to the end user or bystander. For example, if the XR device determines that an individual is moving slower when compared to other individuals who are participating in a competition that requires precision and micromovements and combines that with data related to how often the user uses a particular hand to compete, it is possible that the company may profile the user as "average" for reaction time or precision. If a company buys a data set relating to persons who play said type of games, seeking to employ top players, then this could affect job opportunities for that individual. Moreover, the person would never know. If this information was incorrect or based on a temporary injury that has since healed, the individual is unfairly affected by this inaccurate information.

iv. Misuse

XR technology is being put in place by multiple entities, many of which are unlikely to fully disclose data use and sharing practices.[60] This also means that there may be potential for other individuals or entities to access the data collected or inferred from that data set, some of which may be dangerous or discriminatory to the individuals linked to the data. For example, data on movements could be shared with employers to contest work injuries. Discrete functions of XR technology, such as facial or emotional recognition, could be unethically used to discriminate against individuals who are neurodivergent, have physical disabilities affecting their facial expressions, or come from cultures with physical expressions of emotion that vary from the expressions programmed into the facial recognition technology. In addition, depending on access controls, abusive partners may be able to misuse the information to surveil and further control individuals. For example, an abusive partner could access their partner's XR gaming account and track their partner's location, either by viewing real-time locations or location history. They

[60] *See, e.g.*, Edward Ongweso Jr., *Amazon's New Algorithm Will Set Workers Schedules According to Muscle Use*, VICE (Apr. 15, 2021), https://www.vice.com/en/article/z3xeba/amazons-new-algorithm-will-set-workers-schedules-according-to-muscle-use (highlighting an employer's unforeseen use of biometrics and physical information to manage employees).

could access communication logs or interactions to see who their partner has been engaging with. This information may be used to exert control or as a basis for "punishing" their partner by stalking, harassing, or otherwise abusing their partner, either within the virtual environment or by using the XR information to do so in the physical world. Problems of misuse are already cropping up in the virtual reality experience, such as the recent news article describing an immersive sexual assault experience.[61]

v. Sensitive Categories of Persons, Children, Bystanders, LGBTQIA, and Other Marginalized Persons

Certain privacy risks are heightened based on the category of individual to whom the information pertains. The ability to identify and track a person, constrained only by regulations that are not tailored to XR technologies, poses a heightened risk to children, LGBTQIA, immigrants, religious and racial minorities, and other vulnerable and marginalized persons, such as political or social activists. We discuss the nuances of current regulations for sensitive categories of persons below.

An example of a sensitive category of personal information is health data. XR technology is very likely to collect health information, including any health condition that may affect gait, micromovements, gestures, or facial expression. Collection and use of this data is left to the discretion of the XR company. This enables companies to create massive data sets that make motions uniquely telling and could enable companies to theoretically detect deviations from an individual's expected movements, potentially extrapolating injuries, illnesses, or other medical conditions.[62]

Finally, the technology itself may be more likely to make incorrect assumptions of an individual for reasons out of the individual's control. Various facial recognition algorithms that would likely be used for gesture and facial expression tracking have historically had a much higher rate of incorrect identification on darker skin tones and transgender or non-binary individuals.[63] For example, "emotion

---

[61] *Metaverse Builders Grapple with Sex Harassment Conundrum,* FRANCE24 (Jan. 4, 2022), https://www.france24.com/en/live-news/20220401-metaverse-builders-grapple-with-sex-harassment-conundrum.

[62] Bailenson, *supra* note 11.

[63] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, PROC. MACH. LEARNING RSCH., Feb. 2018, at 1-2; Morgan Klaus Scheuerman et al., *How Computers See Gender: An Evaluation of Gender Classification in Commercial Facial Analysis and Image*

detection" for facial expressions may fail in accurately detecting an emotion and displaying the same during a corporate XR off-site, but only for persons for whom the machine learning model had poor data during training and validation, or persons for whom no data was included during training and validation (e.g., darker-skinned individuals or culturally different individuals).[64] There could be real-world consequences for these individuals in terms of management and career trajectory. This incorrect identification problem may affect individual ability to use XR systems easily, which could impact occupational or educational opportunities, or be used maliciously by the state against the persons affected.

II. LEGAL APPLICATIONS AND POSSIBILITIES

To understand why our existing legal structure does not fully address the risks raised by XR technology, we must first delve into the current system of privacy regulation, control, and enforcement. We have divided the U.S. privacy regulatory system into two parts: private sector and law enforcement. Below, we describe how the current U.S. privacy regulatory system works, its scope, its weaknesses, and possible options for closing enforcement gaps related to XR.

A. Private Sector Regulation

U.S. privacy is generally regulated by a patchwork of sector-specific laws, resulting in coverage gaps where personal data falls through the cracks and leaves individuals without recourse for privacy violations, particularly as relates to new and developing technology. This is certainly the case when it comes to the relationship between XR technology and the privacy regulatory landscape in the U.S. We will examine the current state of private sector privacy regulation in the U.S., identifying where it fails to fully cover risks raised by XR technology. After establishing the current state of potentially applicable privacy laws and identifying gaps, we will discuss some possible solutions for addressing those gaps and the remaining privacy risks inherent in XR technology.

Labeling Services, PROC. ACM HUM.-COMPUT. INTERACTION, Nov. 2019, https://dl.acm.org/doi/10.1145/3359246.

[64] We strongly oppose digital phrenology (also known as emotion detection) and want to make clear that mention of it here is in no way a validation.

1. Current State of Privacy Law Overview

The unique risks presented by XR technology pose a complex regulatory problem. As is frequently the case, technology has developed faster than regulations can keep up, creating gaps in privacy protections and standards for U.S. residents. While industry standards, frameworks, or other self-regulatory mechanisms may help to set expectations for ethical behavior, they are often voluntary by nature and lacking in meaningful enforcement, rendering them unable to act as a substitute for substantial regulation.[65]

Existing U.S. privacy laws address individual rights over personal information, place appropriate restrictions on collecting and using personal information, and impose publicity and notice requirements for personal data breaches, particularly where the breaches include certain data elements. However, these laws are not comprehensive in their protections and do not fully capture the risks posed by XR technology. Several are limited according to geography or sector as well. We briefly discuss some examples of inherently limited statutes below.

- The California Consumer Privacy Act ("CCPA") is solely applicable to California residents, leaving other U.S. residents without the same privacy protections. While companies can opt to use the CCPA as a baseline and extend protections to their entire user population or user base, they are not required to do so and individuals not subject to the CCPA cannot make legal claim to those protections.
- The Children's Online Privacy Protection Act ("COPPA") applies to collection and processing of children's information online. However, these protections apply only to information from children under 13 years of age. COPPA may also protect bystander children under 13 years of age if the company has actual knowledge that the bystander children are under 13. However, this still leaves any children over the age of 13 without protections.
- The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") solely applies to data that is defined as "protected health information" and within the context of processing by covered entities and business associates. Health data or wellness

---

[65] *See* Jedidiah Bracy, *Will Industry Self-Regulation Be Privacy's Way Forward?*, IAPP (June 24, 2014), https://iapp.org/news/a/will-industry-self-regulation-be-privacys-way-forward/; *see also XR Association*, XRA, https://xra.org/ (last visited Nov. 10, 2022); *XR Safety Initiative*, XRSI, https://xrsi.org/ (last visited Nov. 10, 2022); *VR/AR Association*, VRARA, https://www.thevrara.com/ (last visited Nov. 10, 2022).

data that exists outside of the scope of HIPAA is afforded some protections if it falls within the scope of the FTC Health Breach Notification Rule.[66] Note that this does not include genetic information, which falls under the Genetic Information Nondiscrimination Act ("GINA").[67] GINA bars discrimination based on genetic information—however, GINA is not considered a true data protection regulation.[68]

In addition to these statutory regulations, there are also some historically-recognized privacy harms, such as torts of intrusion upon seclusion or public disclosure of private facts. As with the regulations, these are limited in scope and application. Below, we provide a brief summary of many of the existing U.S. privacy regulations and traditionally recognized privacy harms, including the shortcomings of each when applied to XR.

i. The Limited Applicability of Existing Federal and State Statutes

While current U.S. privacy regulations exist at both a state and federal level, these regulations do not constitute full privacy protections. The lack of protections may at times stem from lack of enforcement resources at both the state and federal level. States (Attorneys General) and the Federal Trade Commission are often tasked with investigating allegations of privacy violations and bringing enforcement actions.[69] However, the broad scope of these bodies' remit and the limited resources and staff available can leave individual cases and privacy violations unaddressed due to authorities prioritizing more high-profile cases, allocating resources away from less clear-cut cases that the authorities could potentially lose, or a lack of technical expertise within the groups to take on certain cases.

---

[66] 16 C.F.R. § 318 (2009).
[67] Genetic Information Nondiscrimination Act of 2008, 42 U.S.C. § 2000ff.
[68] *See, e.g.*, Rachele Hendricks-Sturrup, *A Closer Look at Genetic Data Privacy and Nondiscrimination in 2020,* FUTURE PRIV. F. (Mar. 2, 2020), https://fpf.org/blog/a-closer-look-at-genetic-data-privacy-and-nondiscrimination-in-2020/.
[69] *See generally* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy,* 114 COLUM. L. REV. 583 (2014); Chair Lina M. Khan, Fed. Trade. Comm'n, Remarks as Prepared for Delivery at the IAPP Global Privacy Summit 2022 (Apr. 11, 2022) (stating that "the realities of how firms surveil, categorize, and monetize user data in the modern economy invite us to consider how we might need to update our approach further yet.").

Beyond regulatory restrictions, the regulations themselves contain scope limitations that leave broad swathes of individuals unprotected. Many state regulations are not only restricted solely to individuals with residency in that specific state, but also exclude various data types, such as information already covered under federal regulations, like health information, financial data, or entity types (bounded by number of employees, revenue, customer-base size, or explicitly excluding non-profits or other entities). Similarly, federal laws are often limited narrowly to an individual industry area or information type (or may apply solely to particular data elements). While bystander data is not intentionally excluded by existing regulation, it is also not explicitly included. In addition, only one existing statute mentions inferential data, which we will later explore in more detail. This leaves both bystander data and inferential data either unprotected or, at best, in a grey area.

In order to provide a broad picture of the major privacy regulations currently in place, what data or individuals are covered by the regulation, and the specific privacy protections provided, we have created the following chart.[70]

[70] We exclude cybersecurity regulations or security-focused data protection regulations from the scope of this paper to remain focused purely on privacy. We have selected certain state laws that are the strongest examples of their particular type (providing for broad data subject privacy rights, addressing biometric information, etc.). This is certainly not an exhaustive list of state regulations, but we note that any state regulation would not provide comprehensive privacy protections across the U.S. as they are limited to solely that state. For a more detailed list of state privacy regulations, please check the International Association of Privacy Professionals' State Privacy Legislation Tracker, available at https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

Statutes	**Scope**	**Protections Provided**
California Consumer Privacy Act ("CCPA") and California Privacy Rights Act ("CPRA")	Solely personal data of California residents, includes household information and inferential data.[71] Biometric data is also specifically addressed within the regulation.[72]	Together, the CCPA and CPRA provide the data subject rights similar to those under the GDPR: the right to delete,[73] right to access or right to know,[74] right to correct inaccurate information,[75] right to limit use or disclosure of sensitive information,[76] and the right to opt out of the use of automated decision-making technology on personal data,[77] with the addition of the ability to restrict the sale or sharing of personal data.[78]
Electronic Communications Privacy Act of 1986 ("ECPA")	Wire, oral, and electronic communications, including email, telephone conversations, and electronically stored data. Includes data in transit, at creation, and in storage.[79]	ECPA, which updated the Federal Wiretap Act of 1968 and includes both the Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act, prohibits the interception, use, disclosure, or procurement of another person to do so, of any wire, oral, or electronic communications.[80] Interception in this case means accessing the contents of any wire, oral, or electronic communication via electronic, mechanical, or other device.[81] It also protects the contents of

[71] CAL. CIV. CODE § 1798.140(v)(1) (noting that inferential data drawn from personal data elements is, itself, a form of personal data protected under the CCPA).
[72] CAL. CIV. CODE § 1798.140(b) (stating that biometric information includes, among other things, "imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.").
[73] CAL. CIV. CODE § 1798.105.
[74] CAL. CIV. CODE §§ 1798.110, 1798.115.
[75] CAL. CIV. CODE § 1798.106.
[76] CAL. CIV. CODE § 1798.121.
[77] CAL. CIV. CODE § 1798.185(a)(16).
[78] CAL. CIV. CODE § 1798.120.
[79] 18 U.S.C. § 2511.
[80] 18 U.S.C. § 2511(1).
[81] 18 U.S.C. § 2510(4).

		files stored by service providers,[82] and mandates court orders for government use of pen registers and trap and trace devices.[83]
Section 5 of the Federal Trade Commission Act ("FTC Act")	Unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.[84] This applies to all U.S. consumers affected by the applicable methods, acts, or practices.	The FTC is empowered to bring actions against companies or individuals that engage in unfair and deceptive practices.[85] "Deception" includes any representation, omission, or practice likely to mislead a consumer.[86] "Unfairness" includes any act or practice causing or likely to cause (i) substantial injury; (ii) not reasonably avoidable by consumers; and (iii) not outweighed by benefits to consumers or competition.[87]
Illinois Biometric Information Privacy Act ("BIPA")	The biometric information of Illinois residents (explicitly limited to biometrics used to identify an individual).[88]	Biometric information cannot be collected without the written consent of the data subject.[89] In addition, the regulation limits dissemination or disclosure of biometric identifiers or biometric information to solely circumstances where there is consent or where necessary for a specific purpose (acceptable purposes are limited to completing a financial transaction,

[82] 18 U.S.C. § 2701(a).
[83] 18 U.S.C. § 3121(a).
[84] 15 U.S.C. § 45(a).
[85] 15 U.S.C. § 45(b).
[86] Letter from the Federal Trade Commission, Policy Statement on Deception (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.
[87] 15 U.S.C. § 45(n). In addition, a recent Executive Order urged the FTC to, among other actions, exercise rulemaking authority to address unfair data collection and surveillance practices and other areas that inhibit competition and damage consumer privacy protections. Exec. Order No. 14,036, 86 F.R. 36987 (July 9, 2021), at Section 5(h).
[88] Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/10 (including both biometric identifiers (retina or iris scan, fingerprint, voice print, or scan of a hand or face geometry) and biometric information (information based on a biometric identifier and used to identify an individual)).
[89] Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/15(b).

		fulfilling a subpoena or warrant, or as otherwise required by law)[90] and completely prohibits private entities profiting off of individuals' biometric information.[91] Data subjects are granted a private right of action under BIPA and may recover significant fines per violation.[92]
Children's Online Privacy Protection Act ("COPPA")	COPPA applies to the personal information of children under the age of 13 on the Internet or online services (meaning services available over or connected to the Internet).	COPPA has a number of requirements for operators of websites or online services directed at children that wish to collect or process personal data obtained from children. These requirements include providing notice and receiving verifiable parental consent prior to collection,[93] limiting what personal data is collected to what is reasonably necessary for the applicable activity,[94] providing information relating to what personal data is being processed for an individual child (when properly requested by a parent or guardian), and providing opportunity to exercise rights to cease processing.[95]
Family Educational Rights and Privacy Act ("FERPA")	FERPA applies to personally identifiable information of children contained in their education records.	FERPA provides parents with certain rights to review and correct their children's education records and generally requires parents to provide written consent before schools receiving certain federal funds share children's personally identifiable information with other parties.[96] These rights of review, correction, and consent pass to students

[90] 740 ILL. COMP. STAT. 14/15(d) (2008).
[91] 740 ILL. COMP. STAT 14/15(c) (2008).
[92] 740 ILL. COMP. STAT 14/20 (2008).
[93] 15 U.S.C. § 6502(b)(1)(A).
[94] 15 U.S.C. § 6502(b)(1)(C).
[95] 15 U.S.C. § 6502(b)(1)(B).
[96] 20 U.S.C. § 1232g(a).

		once they are over the age of eighteen.[97] Institutions receiving the applicable program funds must inform parents and students of these rights as well.[98] However, several exceptions allow for records sharing in certain circumstances,[99] and this regulation is solely applicable to institutions receiving federal funding under an applicable program.[100]

[97] 20 U.S.C. § 1232g(d).
[98] 20 U.S.C. § 1232g(e).
[99] 20 U.S.C. § 1232g(b).
[100] 20 U.S.C. § 1221(c)(1) (defining applicable program as "any program for which the Secretary or the Department has administrative responsibility as provided by law or by delegation of authority pursuant to law.").

Health Insurance Portability and Accountability Act ("HIPAA")[101]	HIPAA applies to Protected Health Information, which is defined as health information created, transmitted, received, or maintained by the following entities, collectively referred to as "Covered Entities" (not exhaustive): health plans, healthcare clearinghouses, healthcare providers, and their Business Associates who process Protected Health Information on behalf of these Covered Entities.[102]	HIPAA provisions are typically divided into what are commonly referred to as the Privacy Rule and the Security Rule.[103] The Security Rule mandates that covered entities maintain reasonable and appropriate administrative, technical, and physical safeguards to protect the confidentiality of electronic health information in transmission, at rest, and from breaches.[104] The Privacy Rule places limits on how protected health information can be used and disclosed.[105]

ii. Recognized Privacy Harms

In addition to the federal and state statutory privacy protections, the U.S. also has four categories of traditionally recognized privacy torts: intrusion upon seclusion,[106] public disclosure of private facts,

[101] Other federal regulations, such as the Gramm Leach Bliley Act ("GLBA") or the Fair Credit Reporting Act ("FCRA"), regulate data elements, privacy, and security within the financial sector. HIPAA is a portability/data protection regulation, not a privacy regulation specific to privacy rights. However, HIPAA is perceived in the U.S. as a privacy regulation for patient information and has significant privacy impacts, and so we have included it here for that reason.

[102] 45 C.F.R. § 160.102(a)–(b) (2013).

[103] *See Summary of the HIPAA Security Rule*, U.S. DEP'T OF HEALTH & HUM. SERVICES, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited Nov. 11, 2022) , *see also Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUM. SERVICES, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last visited Nov. 11, 2022).

[104] 45 C.F.R. § 164.306 (2013).

[105] 45 C.F.R. § 164.502(a) (2013).

[106] RESTATEMENT (SECOND) OF TORTS § 652B (AM. L. INST. 1977) ("One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.").

appropriation of name or likeness, and false light.[107] Of the four categories, intrusion upon seclusion is the most likely to apply within the XR technology context because of XR technology's erosion of the barriers between public and private spaces. XR brings outside viewers and listeners into the user's private space or, through use of visual and auditory sensors, into the bystander's private space, essentially making those private spaces public. Unlike the other three privacy torts, the mere act of XR technology gathering personal information in an "invasive" manner may be enough to constitute an intrusion upon seclusion privacy violation, because intrusion upon seclusion does not require publication of information or use of information.[108]

Intrusion upon seclusion requires that a party "intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, [and] the intrusion would be highly offensive to a reasonable person."[109] Initially, court decisions related to this tort turned on physical intrusion. The application of the tort has expanded over time to include any type of intrusion into anything the victim would consider private.[110]

While this single privacy tort may be applicable to XR technology in some cases, the ability of existing tort law to meaningfully address digital threats is suspect.[111] Intrusion upon seclusion is generally understood to only protect information that has been kept wholly secret

---

[107] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).
[108] Tigran Palyan, *Common Law Privacy in a Not So Common World: Prospects for the Tort of Intrusion upon Seclusion in Virtual Worlds*, 38 SW. L. REV. 167, 171 (2008) ("Moreover, the other three privacy torts deal with the use of information once it has been acquired. Only intrusion redresses invasions of privacy where the acquired information is not used.").
[109] RESTATEMENT (SECOND) OF TORTS § 652B (AM. L. INST. 1977).
[110] RESTATEMENT (SECOND) OF TORTS § 652B cmt. b (AM. L. INST. 1977) (listing eavesdropping and wiretapping as examples of intrusion).
[111] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 58–59 (2004) (Stating that privacy torts "are not well adapted to regulating the flow of personal information in computer databases and cyberspace."); Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Disclosures*, 11 NW. J. TECH. & INTELL. PROP. 321, 330 (2013) (reading that "torts and their standards regarding information privacy are outdated and have not been adequately adapted to take into account new technologies and their effects on information privacy."); Christopher F. Carlton, *The Right to Privacy in Internet Commerce: A Call For New Federal Guidelines and the Creation of an Independent Privacy Commission*, 16 ST. JOHN'S J.L. COMM. 393, 423 (2002) ("The tort of intrusion upon seclusion and public disclosure is rejected as a solution to online privacy concerns because most of the personal information obtained online is provided voluntarily by the user."); *see, e.g.*, United States v. Charbonneau, 979 F. Supp. 1177, 1179 (S.D. Ohio 1997) (holding that the openness of a chat room diminishes a reasonable expectation of privacy in chat).

previously.[112] This reflects a traditional understanding of privacy in law, where privacy exists solely within entirely private spaces or only where information has been kept private to the point of complete secrecy.[113] Because XR technology blurs the line between private and public spaces and collects vast stores of personal data that include publicly-observable information (such as gait, appearance, or physical location), there is arguably a low probability that a plaintiff could demonstrate complete secrecy and, therefore, receive protection under tort law.

Example: Ryan shares interior decorating tips through an XR service that maps her home space and projects spatial dimensions, such as furniture shape, size, depth, and the same for decorations, colors, or other living space components to an audience. This map is then shared with other users of the XR service, enabling other users to "walk" through the space, overlay parts of the space and features of it onto their own space to compare fit, and identify characteristics and details like paint colors and brands, the source of different furniture and decorative pieces, and other materials used. In a recent image of Ryan's living room captured through the service, the door to Ryan's bedroom was cracked open in the background. Through the cracked door, a user was able to zoom in on some visible objects, including a picture frame in which the framed picture was an intimate picture of Ryan and her fiancée. The user enlarged and distributed the image, using it to shame Ryan for her appearance and to out her as being in a relationship with a woman.

Ryan may argue that the use of the image constitutes intrusion upon seclusion since she did not intend to share the image with a broader audience. However, under existing law, this may not rise to the level of intrusion upon seclusion since Ryan's relationship with a woman is known to certain other people (family, friend groups) and therefore has not been kept wholly secret. More importantly, the element of intentional intrusion into private affairs may be difficult to establish in the XR context. Ryan knowingly allowed the XR app to scan her living room and the inclusion of the visible bedroom and the items inside could be considered part of that choice.

---

[112] *See* Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1354 (Ill. App. Ct. 1995) ("We cannot hold that a defendant has committed an unauthorized intrusion by compiling the information voluntarily given to it and then renting its compilation."); SOLOVE, *supra* note 111 at 59.

[113] Benjamin Zhu, *A Traditional Tort for a Modern Threat: Applying Intrusion upon Seclusion to Dataveillance Observations*, 89 N.Y.U. L. REV. 2381, 2396 (2018) (stating that, under current tort frameworks, "an individual maintains a privacy interest in information that has been kept secret, but that interest evaporates if the information is disclosed or made public").

iii. XR Poses Risks Above and Beyond Those Contemplated by Existing Law

It may appear at first glance that the patchwork of state and industry privacy laws affords users a form of informational privacy that could be leveraged to address privacy concerns in XR. However, as discussed above, the statutes are limited in application. They offer protections only for a specific subset of information or a single geographic jurisdiction, carve out information that is regulated by federal statutes (e.g., HIPAA or GLBA or other primary federal regulators), and often include exemptions for certain entities or operations. Similarly, existing tort law is restricted by the idea that the intrusion upon seclusion must be an "intentional" intrusion into something the victim considers "private" and has kept entirely secret. This may not stand against the test of XR technology, where the private and public distinction is blurred. Taken altogether, the patchwork regulatory system leaves large swathes of individuals and their personal data inadequately unprotected and at the mercy of the processing entities.

Of the statutes explored above, the CCPA incorporates the broadest definition of personal information and also specifies that "inferences" constitute personal data.[114] Though this represents the highest level of privacy protection currently available, it is only applicable to California residents and expressly excludes certain federally-regulated entities and information types.[115] In addition, the CCPA mainly focuses on marketing uses of personal information, imposing few limits on information that may be used for "business purposes" and only applying to personal data processed by for-profit entities.[116] Some may argue that the CCPA and CCPA-like statues would cover XR technology if expanded to residents of other states. However, upon close examination, it is apparent that, even if expanded, the CCPA falls short.

Example: Leah is coming up on her third annual review at her software engineering company, BigTech Co., headquartered in California. During her review, her manager pulls up reports from her most recent two sets of Virtual Reality training results and highlights that, while her performance in the training was successful, her heart rate and blood pressure did not meet the company's established internal benchmarks. According to BigTech Co., the benchmark was set by analyzing data en masse across the company and is a reliable indicator

[114] CAL. CIV. CODE § 1798.140(v)(1)(K) (West 2023).
[115] CAL. CIV. CODE § 1798.145(c)(1) (West 2023).
[116] *Id.*

of the ability to work effectively and efficiently in high stress situations and environments. The evaluation states that Leah's results indicate she will likely be a low performer unable to effectively handle stress and BigTech Co. has decided to suspend any raises, bonuses, or promotion considerations. She is now on a performance improvement plan.[117]

Setting aside the employment law ramifications of the example above as beyond the scope of this paper,[118] we first examine the limitations of Leah's privacy rights under the CCPA. Leah's account or user information within the Virtual Reality training certainly constitutes personal data, as does the information related to her heart rate and blood pressure, which is not only personal data, but could constitute biometric information under the CCPA if used to identify Leah.[119] In addition, under the updates to the CCPA contained in the CPRA, biometric information used for identification is considered "sensitive personal information" and would be subject to additional restrictions and protections.[120]

These rights, restrictions, and protections give Leah the right to see the data, understand if the data is being sold to third parties, and also to rectify incorrect data. They do not give Leah a right to restrict the use of the data within BigTech Co., prohibit decisions made internally on the basis of the data, or challenge the benchmarks or interpretation of the data as indicative of potential.

Let us examine the differences in statutory privacy protections if this scenario took place in Illinois. While it may appear that heart rate and blood pressure would be addressed by a biometric regulation like BIPA, this information is actually not protected since it is neither one of the listed biometric identifiers in the regulation (retina or iris scan,

---

[117] *See* Yuki Noguchi, *Virtual Reality Goes to Work Helping Train Employees,* NAT'L PUB. RADIO (Oct. 8, 2019, 7:18 AM), https://www.npr.org/2019/10/08/767116408/virtual-reality-goes-to-work-helping-train-employees (describing current uses of VR to train employees in the workforce).

[118] We also note that, with the passage of the California Privacy Rights and Enforcement Act of 2020 ("CPRA"), the employee data exemption that allows companies to treat employee data differently than consumers for a limited transitional period of time has been extended to January 1, 2023. This scenario treats employee information as it will be treated once this exemption period ends.

[119] CAL. CIV. CODE § 1798.140(c) (West 2023) (stating that biometric information includes, among other things, "imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.") (Note that what constitutes using the information to identify an individual may vary in interpretation).

[120] CAL. CIV. CODE § 1798.140(ae)(2)(A) (West 2023).

fingerprint, voiceprint, or scan of hand or face geometry),[121] nor is it clearly being used to identify an individual (a requirement to be considered "biometric information" under the regulation). In fact, BIPA explicitly states that "biometric information" does NOT include information derived from items or procedures excluded under the definition of biometric identifiers.[122]

Leah also has limited rights under tort law. It is unlikely that she could successfully claim intrusion upon seclusion, as she cannot claim the information was meant to be wholly secret. Leah potentially could make a claim that the use of the haptics (here, blood pressure and heart rate) to produce a work plan and evaluate her abilities as a worker constitute a physical intrusion and invasion of her privacy, as she was expecting solely to be graded on her performance in the actual substantive training, but by no means is this argument certain to prevail.

Leah's circumstance above demonstrates a significant privacy concern for end users under the current patchwork system of privacy regulations. There are only certain states in which end users are able to exercise any control over how their data is used or collected. Even in those states, these rights are very limited and insufficient in the XR context. The situation is even more problematic for bystanders. Bystander personal data, including images, voice, or other information, will be picked up by XR technology if they are present in the same area that a user is operating the technology.

Example: It's a cool summer evening and Rob is enjoying a cold beer and a virtual poker game with some friends in his driveway, each of them using their head-mounted displays to do so. About 10 minutes into his hangout, he sees someone in his peripheral vision running down his street. Several minutes later, he hears the sound of tires squealing against the pavement. Three weeks go by and he opens his email to find a note that his poker game account data has been requested by law enforcement in connection with an incident in his area on the date of his virtual poker game.[123]

In this scenario, the bystander whose data was picked up in Rob's poker game may have had certain rights to that data, depending on the area. For example, the CPRA update to the CCPA includes a data subject

[121] Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/10 (2008).
[122] *Id.*
[123] *See, e.g.*, Anastasios Nikolas Angelopoulos et al., *Enhanced Depth Navigation Through Augmented Reality Depth Mapping in Patients with Low Vision*, 9 SCI. REPS., 11230 (2019) (describing the use of Augmented Reality depth mapping to aid visually impaired individuals in navigating the real-world environment).

right to deletion where an individual can request that their data be deleted by the company holding that data, subject to certain exemptions.[124] However, in order to exercise this right, an individual must first be aware that the personal data has been collected by the company—why would a person submit a deletion request to a company unless they suspect that it has any of their personal data? In the example above, the bystander would have to have noticed that Rob was using an XR device, recognized that their activities may have been within the range of capture, be able to identify the company behind the XR device, and possibly have additional information required to fulfill the request (for example, information of the date and time of the collection or the account on which the personal data may have been captured). This level of knowledge on the part of bystanders is nearly impossible to meet and unduly burdensome in the rare cases where bystanders may notice the collection and have the information necessary to make the deletion request.

It may also be tempting to try addressing bystander risks under the protections offered under ECPA—however, that is unlikely to prevail. To successfully bring suit under ECPA, a plaintiff must demonstrate that the defendant intentionally sought to intercept content, as defined within the Wiretap Act.[125] First, as mentioned earlier, a bystander may not be aware that their data is being collected, processed or otherwise accessed by an XR company in real-time and know to bring suit. In this case, the bystander would likely be unaware that they were recorded on Rob's XR device. Second, even if the bystander was aware, they would still need to demonstrate standing (injury in fact and violation of a legally protected interest) and, to date, mere access to information has not been sufficient to establish standing.[126] Third, even if a bystander's suit survived Article III standing challenges, the plaintiff/bystander is likely to face challenges in demonstrating intent. If an XR technology company purposefully collects data in real-time to process it and create profiles, then it is likely that a bystander could demonstrate intent.

The distinction between private and public spaces has been slowly eroded over time by various new technologies (e.g., live video streaming). Bystander information collection and processing through XR technology further blurs the distinction. Bystanders in public spaces may have a reasonable expectation that they will be observed by traditional methods, such as CCTV or news videos. However, the amount of individual

---

[124] CAL. CIV. CODE § 1798.105(a) (West 2023).
[125] 18 U.S.C. § 2511(1).
[126] 18 U.S.C. § 2520.

impressions that may be collected in a short period by XR systems and the analysis of these impressions in a big data context are less anticipated. Put simply, bystanders may anticipate casual observation by a human in a public space, but not observation by or through technology that connects the real-time observation to other data about them.[127] Further, bystander data may be collected in spaces such as private businesses, other individuals' private residences, or even the bystanders' residence, if shared with an individual using an XR system.

These examples demonstrate the pitfalls and gaps inherent in the current privacy regulatory landscape for the private sector in the U.S. While certain claims may be possible in individual cases, protections are far from comprehensive and privacy rights often are restricted to certain geographic and industry areas. We now turn to similar coverage gaps in regulations applicable to law enforcement data collection and use.

B. Government and Law Enforcement

1. Existing Law: Reasonable Expectation of Privacy in a Tech World

Fourth Amendment protections struggle to keep up with developing and new technologies as these technologies increasingly blur the line between public and private areas.[128] XR technology exacerbates the problems facing the courts in applying Fourth Amendment protections to novel situations in which these public and private areas are intermingled or overlaid in not only the physical world, but also an alternate reality. XR data is an entire world in which a person can continuously operate and provides an enormous volume of data—from the second-to-second way someone physically moves, to physical and virtual location history, to information as invasive as blood pressure and heart rate. In this section, we'll briefly discuss the *Katz* test for evaluating

---

[127] *See, e.g.*, Mark Sullivan, *The Making of Mojo, AR Contact Lenses That Give Your Eyes Superpowers*, FAST CO. (Jan. 16, 2020), https://www.fastcompany.com/90441928/the-making-of-mojo-ar-contact-lenses-that-give-your-eyes-superpowers (A startup company is making contact lenses that augment a user's reality. These lenses are not easily identifiable by bystanders, and the device privacy policy is not publicly available on Mojo's website, although there is a contact email address to acquire the same. We did not request this policy.).

[128] *See* Ellysse Dick*, How to Address Privacy Questions Raised by the Expansion of Augmented Reality in Public Spaces,* INFO. TECH. & INNOVATION FOUND. (Dec. 14, 2020), https://itif.org/publications/2020/12/14/how-address-privacy-questions-raised-expansion-augmented-reality-public/ (Ellysse Dick reviews the history of technology changing the balance between public and private over time and makes policy recommendations for augmented reality in public spaces.).

Fourth Amendment protections for direct government searches and the privacy risks inherent in XR under *Katz*. From there, we will move to *Carpenter* and the third-party doctrine.

Fourth Amendment law purportedly balances protecting the right of people to be secure from unreasonable searches with law enforcement evidence-gathering and investigation procedures.[129] When examining Fourth Amendment protections, the courts assess whether a search by law enforcement abrogates the "reasonable expectation of privacy" discussed in *Katz*.[130] If the court does not find that a reasonable expectation of privacy exists, then it concludes that the search is reasonable and a warrant is not required. While the Fourth Amendment is generally presented as protecting a "reasonable expectation of privacy," a closer examination of Fourth Amendment case law demonstrates that "privacy" is frequently entangled with concepts of ownership and property rights.[131] This conflation of privacy with ownership or property has ushered in an understanding that "private" spaces are those that are privately owned or controlled. The way in which *Katz* has been applied creates a scope problem for Fourth Amendment protections as technological developments increasingly bring the public sphere into private spaces and change what we find to be "reasonable" for privacy expectations in public spaces.[132]

Example: Eliza is suspected of trafficking controlled substances, but authorities do not yet have enough information for a warrant. Eliza is playing an XR massively multiplayer online role-playing game (MMORPG) that incorporates players and their surroundings into the game using headgear and motion sensors placed around the room. Anyone above the age of 13 years can play this game from any part of the world. Eliza likes to play with a background

---

[129] Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 861 (2004) (describing the goal of the Fourth Amendment rules as "a rule-structure that simultaneously respects privacy interests and law enforcement needs").

[130] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (presenting a two-part test in which there must be an actual (subjective) expectation of privacy, and society must be prepared to recognize that expectation as reasonable).

[131] *Id.*; *see also* Sherry F. Colb, *A World Without Privacy: Why Property Does Not Define Limits of the Right Against Unreasonable Searches and Seizures,* 102 MICH. L. REV. 889, 894 (2004) (describing how historically "protecting property . . . has in the past largely encompassed protecting privacy as well").

[132] While we do not address this concept here in this paper, it appears to us there is also simultaneously a thread of broad discretionary authority for the government in its law enforcement capacity, similar to allowances for general warrants, that sneaks its way into the gaps left by the way the courts have currently addressed Fourth Amendment issues in the technology space.

masking filter for location protection. Eliza does not notice that her filter is glitching out whenever she interacts with an object in the game.

The FBI finds out that Eliza is an active player of the MMORPG. An undercover agent poses as a fellow player in the game and observes during gameplay that Eliza has what could be suspicious paraphernalia in a basket when the filter glitches out during a fight between members of the party and several werewolves.

The FBI wants to use a series of screenshots that they have taken from the game which show the suspicious paraphernalia as evidence in the case they are building against Eliza. They contend that their prior actions in obtaining the screenshots are not a warrantless search because Eliza intentionally broadcasted her home to the public by playing the MMORPG and they had lawful right of access to the paraphernalia by virtue of being game players.[133] They argue that the objects they saw were suspicious paraphernalia in plain view.[134] Eliza's attorney argues that her home is not a public space, that Eliza deliberately sought to protect the details of her home from other players to maintain her home as a private space, and that the undercover agent's viewing and screenshots fall outside the scope of the plain view doctrine and instead constitute a warrantless search in violation of the Fourth Amendment.[135]

---

[133] For the purposes of this section, we are setting aside the application of the third-party doctrine, which we will address later in this section; *see also* Dick, *supra* note 128 (describing how augmented reality technology may exacerbate privacy concerns, allowing the public into what were previously considered private spaces and essentially collapsing the boundaries between the two).

[134] Under existing criminal procedure doctrine, evidence in the "plain view" of an officer who has a right to be in a location allowing them to perceive the evidence can gather the evidence without a search warrant. Washington v. Chrisman, 455 U.S. 1, 9–15 (1982) (explaining that an officer lawfully in the dorm room may seize marijuana seeds and pipe in open view). This is the plain view doctrine and is limited by probable cause (e.g., the officer must have probable cause to believe that the items in plain view are contraband).

[135] *See* Ogletree v. Cleveland State University, No. 1:21-cv-00500, 2022 WL 3581569, at *24 (N.D. Ohio Aug. 22, 2022) (The court granted plaintiff's motion for summary judgment, finding that a remote proctoring software room scan of plaintiff's bedroom was an unreasonable search under the Fourth Amendment. The Court dismissed defendant's argument that plaintiff did not have a reasonable expectation of privacy from the room scan in his house, noting "[r]ooms scans go where people otherwise would not, at least not without a warrant or an invitation."); Joseph Cox, *FBI Asked Sony for Data on User Who Allegedly Used PlayStation Network to Sell Cocaine*, VICE (Dec. 3, 2019, 5:24 PM), https://www.vice.com/en/article/zmjp73/fbi-asked-sony-playstation-4-user-data-cocaine-dealer (FBI requests information about PlayStation 4 player's email, chat, game progress, and account interactions in drug investigation).

Under the *Katz* test, it is possible that the court will find: (1) that the screenshots fall within the scope of the plain view doctrine *if* they consider lawful right of access to include viewing Eliza's home through the XR game space instead of actual physical access and acquisition; and (2) that Eliza's participation in the MMORPG is a "knowing exposure" of her home to the FBI and removes her privacy protections for her home. There is also a far-fetched possibility that the court will consider Eliza's attempt to mask her physical reality sufficient to give a head nod to the *Katz* test of a reasonable expectation of privacy and choose to protect the idea of privacy in one's home under property theories.[136] This is an oversimplified example of the struggle that a court applying *Katz* is likely to experience when determining how to protect XR data.

There is substantial debate regarding the nature of the right to a reasonable expectation of privacy, with many eminent scholars arguing that the Fourth Amendment is not the ideal basis for protecting privacy.[137] We agree. Decisions using the *Katz* test, centered on a reasonable expectation of privacy, have resulted in situational rules that seem to only meaningfully protect privacy where information is "private from public perception" or concealed from potential public exposure, leaning into an idea of synonymous privacy and secrecy instead of into a test that equips courts to meaningfully evaluate a reasonable expectation of privacy.[138]

As one might imagine, cases involving analyses of "reasonable expectations" of privacy typically hinge on "knowing exposure" and the

---

[136] Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

[137] Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1519–21 (2010) (capturing perspectives on the circular nature of the reasonable expectation of privacy test and also on the difficulty in determining what is normatively reasonable for society); *see, e.g.*, Matthew Tokson, *The Normative Fourth Amendment*, 104 MINN. L. REV. 741, 742 (2019) ("The test is tautological, incoherent, ignores important Fourth Amendment values, gives judges free reign to impose their policy preferences, and, as a practical matter, is notoriously unhelpful. It has failed to protect privacy in many digital forms of information, will shrink the Fourth Amendment's scope as knowledge of privacy threats increases, and is increasingly useless in the Internet age.") (internal citations omitted).

[138] *See* Woodrow Hartzog, *The Fight to Frame Privacy*, 111 MICH. L. REV. 1021, 1027–28 (2013) (using Fourth Amendment law as a key example in which "[t]aken to the logical conclusion, the secrecy paradigm forces a choice between living the life of a hermit or relinquishing our privacy and, in turn, a key protection against excessive government surveillance").; *see also* Kerr, *supra* note 129 (contrasting various lines of Fourth Amendment cases, such as searches of the home, closed containers, and surveillance law, and identifying the different procedures found in each).

definition of "public."[139] The public may be surprised to know that putting garbage out for the city to collect and dispose of is the same as exposing the contents publicly, allowing any law enforcement officer to go through the trash (no warrant or exception needed, no search involved).[140] Or, as in *Ciraolo*, even if you have a privacy fence around your house, if law enforcement were to fly above the house and view anything problematic within your privacy fence, it is still considered publicly exposed and not protected by warrant or probable cause requirements—regardless of whether you had taken steps, like the fence, to mitigate the risk of it being public to any average viewing perspectives.[141] The courts' strange interpretations of "public exposure" include that one has no reasonable expectation of privacy from surveillance or GPS tracking if you are in a vehicle off of your private property.[142] Then, of course, there are the later in time, more tech-focused decisions in *Kyllo*, *Jones*, and *Carpenter*, which bring us back to one of the core questions posed by the creation and adoption of XR technologies—what is public and what is private for the purpose of Fourth Amendment protections?[143]

---

[139] Katz, 389 U.S. at 351–52; Colb, *supra* note 131 (describing the development of Katz and the way that courts approach the "reasonable expectation of privacy" in a search).
[140] *See* California v. Greenwood, 486 U.S. 35 (1988) (Law enforcement searched through Greenwood's trash bags twice after Greenwood placed the trash on his curb for trash pick-up and seized illegal content. The Court found that this did not violate the Fourth Amendment because of the public accessibility of the trash bags and Greenwood's intent to convey the trash to the trash collector, a third-party.).
[141] *See* California v. Ciraolo, 476 U.S. 207 (1986).
[142] *See* United States v. Knotts, 460 U.S. 276 (1983) (Law enforcement embedded a radio transmitter in a container of chloroform Knotts had ordered from a third party so law enforcement could track the container movement. The Court held that there was not a reasonable expectation of privacy for the container's movement or for the surveillance of the car, while publicly viewable, carrying the container. While the opinion was unanimous, the concurrences marked a wariness to greenlight "augmenting" law enforcement capabilities, and concerns around whether the application of the radio transmitter was truly not a privacy intrusion. The case did not reach the question of whether this was a search under property law because the radio transmitter was added prior to Knotts' possession); *see* United States v. Karo, 468 U.S. 705 (1984) (The installation of a beeper by the DEA in a can the DEA owned prior to being passed off by a confidential informant to a potential suspect was neither a search nor a seizure, however monitoring the beeper while it was within a private residence and not publicly viewable was a search for some of the defendants.).
[143] Kyllo v. United States, 533 U.S. 27, 29 (2001) (considering whether warrantless thermal imaging of a home is a search in violation of the Fourth Amendment); United States v. Jones, 565 U.S. 400, 402 (2012) (considering whether attaching a GPS tracker to the bottom of a car without a warrant and tracking it onto private property is a search in violation of the Fourth Amendment); Carpenter v. United States, 138 S. Ct. 2206, 2214–15 (2018) (considering whether cell site location information (CSLI) collected without a warrant from a third party is a search in violation of the Fourth Amendment).

The distinction is particularly important in an XR-enabled world where employers, healthcare entities, leisure activity providers, education entities, and other industries can choose to provide XR technology that requires a person to provide access to places that were previously private in order to participate in a desired or necessary activity. For example, a dance school may offer students XR-enabled classes using avatars. Perhaps instead of a traditional studio, the courses will be taught in each instructor's personal home studio. Assuming the technology maps more space than solely the studio within the instructor's home, has the instructor knowingly publicly exposed their entire home? For how long? How much data is law enforcement entitled to obtain through this technology? Under *Katz*, the answer is unclear. Perhaps solely the studio will be considered knowingly publicly exposed and the rest of the home would remain a constitutionally protected space that is unknowable without physical intrusion and, therefore, protected under the later decision in *Kyllo*, which we will discuss below. Conversely, perhaps the map of the home—both studio and the remaining rooms/property—will be considered part of the employer's property and not a constitutionally protected area.

2. Moving Away from *Katz*? Fourth Amendment Law Tackles Technology

When the physical and technological realms were more clearly delineated and, in turn, public versus private spheres were more clearly delineated, the pre-*Katz* approach to balancing privacy and law enforcement needs appeared functional. But when new technologies were introduced that blurred the private-public distinction, this balance shifted. It more heavily favored law enforcement needs and *Katz*'s reasonable expectation of privacy test fell apart.[144] Even in *Kyllo*, where the Court grappled with privacy considerations as applied to a new technology and subsequently developed a test that expanded upon a reasonable expectation of privacy, the Court attempted to hold onto the idea of a "home" as inviolable.[145]

In *Kyllo*, law enforcement used a thermal-imaging device trained on a suspect's home to see if the thermal readings would provide evidence

---

[144] *See* Katz, 389 U.S. 347 at 361 (setting forth the test that law enforcement investigations that violate a reasonable expectation of privacy are unconstitutional unless there is a warrant or other exception).
[145] Kyllo, 533 U.S. at 40.

that the person was growing marijuana inside his house.[146] The Court held "[w]here . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[147] While intended to accommodate the development of new technologies, the decision in *Kyllo* hinges on two factors that when applied do not cleanly provide privacy protections for new technology. According to the Court,

> obtaining by sense enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area," *Silverman*, 365 U. S., at 512 . . . constitutes a search at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.[148]

In the first factor, the Court circumscribed the government's use of devices or technologies to those devices or technologies that are "in general public use." Taken to its logical conclusion, it is possible, though unlikely, that the Court can choose to find that this exact search would be appropriate without a warrant in the event that thermal-imaging technology use becomes widespread and, thus, in general public use. As a second factor, the Court considered whether the thermal reading by the device that enabled law enforcement to conclude that Kyllo had grow lamps for marijuana within the house was information that would "previously have been unknowable without physical intrusion" into a constitutionally protected area. This second factor is dead on arrival in the XR-enabled world where private companies are focused on "erasing the borders between digital and physical" such that physical intrusion will not be required to actually know the layout and content details of an area. While in *Kyllo* the police were using a thermal imaging device from outside the home, XR, if adopted across the general public,[149] will create situations in which users will have to enable "public" access to areas that

---

[146] *Id.* at 29–31.
[147] *Id.* at 40.
[148] *Id.* at 35.
[149] *The Future of Extended Reality*, SKIDMORE CONSULTING GRP., https://skidmore-consulting.com/resources/the-future-of-extended-reality/ (last viewed Aug. 27, 2022) (stating that "extended reality market projected to grow from $42.55 billion in 2020 to $333.16 billion by 2025").

"would have previously been unknowable without physical intrusion" in order to participate in society—including in areas such as workforce training, healthcare visits, education, and more.[150] Physical intrusion will not be necessary in XR instances where companies build entire environments using real-world existing physical characteristics (wind, ambient noises, voices), combined with haptics (smells, sensory feedback for touch) and near real-life avatars or projections of people—the intrusions can be much simpler and be accomplished with the aid of the XR companies.[151] As we will explore later in this paper, it is possible for technology companies to implement design choices that are more privacy-protective and help mitigate this risk.

For at least two reasons, it is likely that a court confronted with an XR-enabled society will consider observations in the XR environment to be lawful searches if they continue to use the reasonable expectation of privacy standard and its offshoots. First, XR will at that point likely be in general public use and the mapping will be novel in a way that defies comparisons made to the "physical intrusion" context. Second, some courts will likely consider using XR-devices or programs to fall within the "third party doctrine," a much-criticized doctrine that we'll address next. It is also entirely possible that a court confronted with an XR-enabled society will continue to draw tortured comparisons to non-technological situations and provide protections to individuals participating in mapped versions of previously constitutionally protected places that exist in the physical, real world. It is equally likely that such comparisons will leave significant gaps and continue the trend of fact-based or situational attempts at protecting privacy through the Fourth Amendment.

Would enabling XR devices to cross-map your reality for the game be the same thing as inviting or trusting a law enforcement person with the details of your home?[152] Will the court carve out areas that are XR

---

[150] *See* Hartzog, *supra* note 138 at 1027–28 (reviewing Daniel Solove's "Nothing to Hide: The False Tradeoff Between Privacy and Security" and declaring that "[T]he secrecy paradigm forces a choice between living the life of a hermit or relinquishing our privacy, and in turn, a key protection against excessive government surveillance").
[151] Sebastian Veldman, *Extended Reality: A New Window in the Digital World*, ACCENTURE INSIGHTS (Mar. 22, 2018), https://www.accenture.com/nl-en/blogs/insights/extended-reality-a-new-window-on-the-digital-world; Jennifer Langston, *"You Can Actually Feel Like You're in the Same Place": Microsoft Mesh Powers Shared Experiences in Mixed Reality*, MICROSOFT: INNOVATION STORIES (Mar. 2, 2021), https://news.microsoft.com/innovation-stories/microsoft-mesh/ (Microsoft introduces Mesh mixed reality functions in office workspaces and medical workspaces).
[152] Hoffa v. United States, 385 U.S. 293 (1966) (finding no Fourth Amendment violation where a confidential informant, trusted by the defendant, remained in the defendant's hotel room while the defendant spoke to his attorneys and shared that

enabled from areas that are blocked from view by physical items?[153] Will the court revisit the "informed consent" used for terms and conditions or click-wrap license agreements, modify it for XR, and determine that societal expectations (here, user expectations) about XR software or hardware can protect "private" spaces or otherwise provide a "reasonable expectation of privacy?"

As we examine the potential interplay between XR technology and existing Fourth Amendment law, it appears very likely that continuing to apply *Katz*, in which the Court referenced "knowing public exposure," will undercut the right to privacy in an XR-enabled society. Even if an XR technology does not seek to map the inside of a home, that same technology can still capture, share, retain, analyze, transmit, and use a house layout, down to the smallest detail, effectively making what was previously a private space knowable to private companies.[154] Furthermore, participation in a society where employment, healthcare, leisure, and general existence moves into various XR environments owned by various private companies will subject a person to being knowable and "in public" or, alternately, knowable and to have made a "choice" to provide information to a private company, with that information then subject to the third-party doctrine.

3. Third Party Doctrine

Prior to 2018, law enforcement could acquire data about individuals from third parties with no limitations or considerations for the individual's "reasonable expectation of privacy." This was true even if the individual assumed that the information wouldn't be redisclosed. The only restrictions on what a third party could disclose were voluntarily created or undertaken by the third party and often dictated by the third

---

information to the government); United States v. Garcia, 997 F.2d 1273 (9th Cir. 1993) (finding no Fourth Amendment violation where police officers posing as apartment hunters arrived at the back entrance of a person's home and saw the person using cocaine).

[153] *See* Maryland v. Macon, 472 U.S. 463, 469 (1985) (Law enforcement may enter a public store front while posing as a customer for the purposes of law enforcement but may not enter areas that are only accessible for employees.).

[154] Roberto Baldwin, *Google Maps' AR Adds Navigation Hints to the Real World,* ENGADGET (Feb. 11, 2019, 3:41 PM), https://www.engadget.com/2019-02-11-google-maps-ar-directions.html (Google Device engaged in reality mapping with AR); *see* Solarflare Studio, *BP Future - Magic Leap Experience*, YOUTUBE (Feb. 1, 2020) (demonstrating a Mixed Reality use of a Virtual Reality headset in which an engineer is manipulating various items within the virtual layout of a space from the comfort of his own home).

party's terms of service, privacy policy, or other internal processes or policies. This was the result of the Third Party Doctrine, first set forth by the Supreme Court in 1976.[155] In the XR environment, the doctrine would easily allow a company to provide any of the following types of data to law enforcement:

- Physical body movements and patterns: hands, eyes, head, gait, full body tracking, responses to haptics
- Environment and surroundings: sound, visuals, detailed location maps
- Biometrics: blood pressure, pulse oximetry, respiration, voice prints, face prints, iris recognition
- Geolocation: This may be detailed or generalized geolocation information.
- Device Information: The types of devices used and how they are connected.
- Behavioral Patterns: Similar to social media, this would include who people interact with, how often, and how they interact.
- Bystanders: physical traits, potentially biometrics, any recorded audio or video, and location information

This is not an exhaustive list by any means and raises the same questions that have been raised many times before by privacy scholars—what happens when this data is combined with other data from data brokers? What will the information reveal? How thoroughly is an individual tracked?[156] It seems that the Supreme Court is cognizant of the troubles posed by advances in technology and the continuation of the third party doctrine and has accordingly expanded Fourth Amendment protections with new technology developments in mind.[157] In a recent case, *Carpenter v. United States*, the Court held that law enforcement's request for cell site location information from the cell company for a

[155] United States v. Miller, 425 U.S. 435, 443 (1976).
[156] *See Surveillance city: NYPD can use more than 15,000 cameras to track people using facial recognition in Manhattan, Bronx and Brooklyn,* Amnesty International (last viewed Aug. 27, 2022) https://www.amnesty.org/en/latest/news/2021/06/scale-new-york-police-facial-recognition-revealed/ (Law enforcement data sets that can be combined with XR-enabled device information).
[157] JOSEPH JEROME & JEREMY GREENBERG, AUGMENTED REALITY + VIRTUAL REALITY: PRIVACY & AUTONOMY CONSIDERATIONS IN EMERGING, IMMERSIVE DIGITAL WORLDS at 18 (Future of Privacy Forum, Apr. 2021), available at https://fpf.org/wp-content/uploads/2021/04/FPF-ARVR-Report-4.16.21-Digital.pdf (Noting *Jones*, *Carpenter*, and *Riley* appear to recognize protections for certain granular types of data despite provision to a third party, and that certain data sets "reveal much more in combination than any isolated record.").

seven-day period constituted a search under the Fourth Amendment because of the depth and breadth of the data this type of request would produce.[158] The Court reached this decision under the *Katz* test, aided by several factors, such as volume of data, the sensitivity of the data (what it reveals about a person), and "the inescapable and automated nature of its collection."[159] Since *Carpenter*, Fourth Amendment scholars have found that lower courts have applied a mix of the "reasonable expectation of privacy" test and the factors set forth in *Carpenter* to determine whether information is protected by the Fourth Amendment, both in cases that would normally be third party doctrine cases, and in cases of direct government surveillance.[160] If courts continue to adopt *Carpenter* for both third party doctrine and direct government surveillance, there is a decent chance that XR technology data will be better protected from Fourth Amendment searches that are at odds with a person's expectation of privacy in their data than XR data would otherwise be under the *Katz* test.

While we wait and see where the Fourth Amendment search cases will go next, we cannot lose sight of the fact that judicial opinions and decisions are, for the most part, retrospective. The harm to an individual will have already occurred before the case arrives in front of a judge, and privacy harms are for the most part, irreparable harms. Instead of waiting for such harms to occur, we encourage both legislators and technologists to act first.

C. Solving for Privacy in the XR-Enabled Environment

There are two possible options we see to address current XR privacy issues. First, legislators could pass new legislation or amend existing legislation to address the existing gaps in privacy regulations. These legislative efforts ought to recognize XR-specific privacy harms

---

[158] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).
[159] *Id.* at 2223 (The Court specifically held that "In light of the deeply revealing nature of [cell site location information], its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection."); *see also* Matthew Tokson, *The Carpenter Test as a Transformation of Fourth Amendment Law,* UNIV. ILL. L. REV. (forthcoming 2022), available at https://ssrn.com/abstract=4094166 (Tokson sums up the *Carpenter test* as follows: "The revealing nature of the data collected; the amount of data collected; and whether the suspect voluntarily disclosed their information to others." We also recommend reading this paper for an up to date and in-depth treatment of *Katz* and *Carpenter*, as well as for the proposal that the *Carpenter* factors replace the *Katz* test entirely.).
[160] Tokson, *supra* note 159, at 20–23.

and provide protections and remedies for individuals. Second, courts could address the gaps in privacy protections by using case law to expand existing regulations to include XR cases. Practically, the first of these is most likely to prove effective. For this reason, we focus on legislation below and briefly address the potential for courts to bolster privacy and the possibility of XR industry standards.

1. Legislative Solutions

The most promising potential approach to addressing regulatory gaps in privacy protections related to XR technology is through passing updated privacy regulations.[161] Ideally, these updated regulations will strive to be technology neutral with a scope of protections expansive enough to address risks associated with new technologies as they develop and mature. As mentioned earlier in this paper, U.S. privacy law protecting the privacy of personal data in many cases is often limited in scope, applying either on a state-wide or industry basis. However, new regulations need not necessarily follow this trend and could be implemented at the federal level, joining federal regulations that are somewhat broader in scope, such as ECPA or the CFAA. Alternately, regulation could be introduced that incorporates existing privacy law and updates certain portions of those laws for more complete regulatory coverage. Regardless of scope, effective regulation that addresses privacy risks of XR technology should include certain measures. We briefly touch upon inclusions that must be present in any effective XR privacy legislation.

i. Definitions

Personal Data

First, a regulation that effectively addresses privacy risks in XR technology must have a clear definition of personal data.[162] Current regulations can vary widely in their definitions of personal data, in particular when a law is specific to an industry or group.[163] While it is generally agreed that information which clearly identifies an individual

---

[161] *See* JEROME & GREENBERG, *supra* note 157, at 22.

[162] Note that even the agreed-upon term varies across regulations: "personal data," "personal information," and "personally identifiable information" all act as variants without delving into the more sensitive forms of personal data.

[163] *See, e.g.*, Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (2006); Gramm-Leach Bliley Financial Modernization Act, 15 U.S.C. §§ 6801–6809; Video Privacy Protection Act, 18 U.S.C. § 2710.

(such as name, address, or phone number) is considered personal data, some regulations are much more expansive (including taking cues from the GDPR definition, which includes "any information . . . related to an identified or identifiable natural person," or expanding the definition to include information that could be linked, directly or indirectly, to an individual *or household* under the CCPA). Many regulations no longer consider information to be personal data if it is "fully anonymized," though the standard for anonymization varies, and some experts have demonstrated that it may not actually be possible to render any personal information completely anonymous.[164] Regulations may also have exclusions for data covered by other privacy regulations.[165]

In order for any new regulation to fully address the privacy challenges raised by XR technology, we propose that its definition of personal data must include both identified and identifiable data (meaning, both data that on its own identifies an individual and data that could, in combination with other data, be used to identify an individual).[166] This distinction would include anything short of fully anonymized data that cannot through any combination or reidentification method be linked to an individual. The definition must explicitly include both inferences made from personal data and pseudonymized data.[167]

XR Technology

In the event that legislators choose to draft regulation that specifically addresses XR technology, there must be a clear definition of what constitutes extended reality to avoid inadvertent loopholes for XR or other technologies from which legislators seek to proactively mitigate privacy risks. For example, the Extended Reality Association (XRA) adopts a broad definition and defines XR to include AR, VR, MR (also defined terms), and "other forms of alternate, expanded, or immersive reality applications, including those not yet invented."[168] The Extended Reality Safety Initiative (XRSI) considers XR to be "a fusion of all the realities—including Augmented Reality (AR), Virtual Reality (VR), and

---

[164] Paul Ohm, *Broken Promises of Privacy*, 57 UCLA L. REV. 1701, 1737–38 (2010).
[165] *See* California Consumer Privacy Act, CAL. CIV. CODE § 1798.130 (exemption for information covered by HIPAA, GLBA, FCRA, and other federal regulations).
[166] *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1817 (2011).
[167] Pseudonymized data is not meaningfully masking the identity of an individual in XR technology considering the volume of data points collected and the analysis, combination, and compilation abilities of the technology processing those data points.
[168] *XR at a Glance*, XRA ASS'N, https://xra.org/xr-at-a-glance (last visited Aug. 27, 2022).

Mixed Reality (MR)—which consists of technology-mediated experiences enabled via a wide spectrum of hardware and software, including sensory interfaces, applications, and infrastructures."[169] Unlike the XRA definition, this definition doesn't clearly define AR, VR, or MR. We recommend that legislators adopt a definition that at the very least defines the core terms (AR, MR, VR, immersive realities) and is scoped broadly enough to include hardware and software directly connected to the use, provision, or support of AR, MR, VR, and other immersive realities.

ii. Consistency, Correlation, Conformity

Legislators should take care to ensure that proposed legislation incorporates or references (and does not reduce) existing privacy protections. For example, where a business associate uses an extended reality technology that may access and use PHI, any new privacy regulation should not undermine the protections afforded by HIPAA or stymy the portability and sharing of PHI specifically permitted by HIPAA. Legislators may also choose to help bring the U.S. into step with the privacy regulatory environment abroad by adopting requirements that technology companies provide stronger protections for sensitive data ("special categories of data" as defined by GDPR).[170] This would both make the companies developing these technologies competitive on the international stage and also provide greater protections to the end users.

iii. Privacy Principles

Legislators may also choose to include several "privacy principles"—basic requirements of privacy frameworks that exist in the U.S. and internationally that provide clear guardrails for companies developing XR technology. There are some slight variations on the principles throughout the world, but many remain consistent.[171] For

---

[169] *Extended Reality (XR)*, *supra* note 25.
[170] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 38.
[171] *See, e.g.*, *Ten Principles of Privacy Protection*, BRITISH COLUMBIA, https://www2.gov.bc.ca/gov/content/employment-business/business/managing-a-business/protect-personal-information/principles (last visited Aug. 27, 2022); Ann Cavoukian, *The 7 Foundational Principles*, PRIV. BY DESIGN (last modified Jan. 2011),

example, the NIST Privacy Framework subcategories include (1) assessing data inputs and outputs for bias, (2) limiting observability and linkability of data (increasing dissociability), (3) limiting inferences, and (4) enabling end users to have control over the processing of their data.[172] The OECD framework includes concepts such as (I) data minimization, (II) data accuracy, and (III) individual data rights (transparency and rectification).[173]

Ideally, a privacy-focused regulation that will impact XR will include requirements addressing the following, pulled from privacy principles across the world:

- Transparency - Individuals must be clearly able to understand the types of data collected from them, the derivative data that may be developed, the purpose of the collection, use, or development, and to where that data is or may be transferred or sold. Individuals should also be informed of and able to understand any automated decision-making processes based on their data (e.g., explainable artificial intelligence).
- Choice - End users must be able to opt-in or opt-out from further collection, use, development, or sharing or sale of their data. This could be granular or it could be at high-level categories. Users must also be able to refuse any data processing not necessary for delivery of the services or use of the technology. The strongest standard would be that any data use that is not strictly necessary be opt-in only.[174]
- Individual Rights - End users must be able to obtain copies of their data, including derived data, correct their data if it is incorrect, and have their data deleted. They should also be able to contest automated-decision making practices based on their data (including inferences).
- Risk Assessments - Companies must be required to assess the impact of the way they plan to collect, use, share, sell, or create personal data (derived or other) and implement greater privacy and/or security controls (including granular opt-in/opt-out) for

---

https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf; Regulation (EU), *supra* note 170, at 35.

[172] U.S. DEP'T OF COM., NAT'L INSTITUTE OF STANDARDS AND TECH., NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT VERSION 1.0 (2020).

[173] *See* Ben Gerber, *OECD Privacy Principles*, OECD, http://oecdprivacy.org/ (last modified Aug. 9, 2010).

[174] *See* discussion *supra* note 12.

higher risk data impacts (and higher risk data) or abstain from those data processing practices where risks cannot be mitigated.

- Data Minimization and Retention - Companies should carefully consider the amount of data they collect and otherwise process and lean towards only having purpose-driven collection with robust deletion policies so that they do not hoard databases filled with data.
- Dark Patterns - Companies must be barred from using dark patterns or manipulative design (e.g., forced continuity on subscriptions or user interfaces that automatically opt users into the most disclosure of personal data).
- Bystander Data/Environmental Data - The company must actively engage privacy-protective technology for non-end users and must not collect environmental data where the data may include minors or vulnerable populations (e.g., pregnant women, LGBTQIA+ persons). This would be something companies would assess and tailor depending on the environment in which the technology is deployed.
- Law Enforcement - Requests for data held by companies must require a warrant for law enforcement to be able to access the data.

iv. Bystander Data

As noted above in the example where bystander information is picked up in Rob's XR poker game, XR technology is able to pick up bystander information both in greater volumes than may be reasonably anticipated and within spaces the bystander may believe to be more private than public. In addition, bystanders have a much greater challenge before them to exercise any rights they may have in their personal data. Proposed regulations should take into consideration bystander risk and enshrine bystander rights. Possible approaches to establishing privacy rights for bystanders could include technical fixes, such as mandating XR technology automatically blur or distort images or audio of bystanders (non-direct persons), or administrative fixes, such as notice-based data collection and deletion. Another possible approach is requiring XR companies to provide publicly available data subject request options. However, we note that the first listed option is preferable, since requests to delete still place too much onus on bystanders to locate XR companies and proactively seek out whether their information has been collected—at a high cost of time, information, and effort.

v. Enforcement and Remedies

Legislation would be incomplete without meaningful enforcement against violations of statutory requirements. Any effective XR regulatory scheme must indicate what body—either existing or created within the regulation—will be tasked with ensuring that requirements are met and violations penalized. Effective enforcement is necessary both to serve as a disincentive for businesses to ignore or improperly fulfill legal obligations and as a bulwark for individual privacy rights. Remedies for violations, such as monetary penalties, payment to individuals negatively affected, public notification, or other legal actions, must also be explicitly accounted for within the regulation.

vi. Private Right of Action

Enshrining private rights of action in proposed XR technology regulations could serve several privacy and safety purposes. For example, a private right of action could function as a means to more fully empower the individual to have more control over their personal data. If individuals are able to bring suit for improper collection or use of their information, sharing without permission, or other potential misuse, it gives those individuals more say over their information and may prompt more engagement from individuals with the collection and use of their personal information.

In addition, a private right of action serves as a way to spread enforcement obligations and counteract the limited resources of many enforcement bodies and agencies to pursue regulatory violations. Many agencies and enforcement bodies are unable to pursue every privacy violation due to time and resource restrictions and competing priorities.[175] A private right of action would serve as an additional incentive for companies using XR technology to strictly follow regulatory requirements. In the interest of avoiding potential lawsuits related to breaches, misuse, harms, or other causes, companies are more likely to adopt risk-mitigating practices, such as data minimization, anonymization, strong security measures, and more.

---

[175] *See* Joseph Jerome, *Private Right of Action Shouldn't Be a Yes/No Proposition in Federal Privacy Legislation,* INT'L ASS'N PRIV. PROFESSIONALS (Oct. 3, 2019), https://iapp.org/news/a/private-right-of-action-shouldnt-be-a-yes-no-proposition-in-federal-privacy-legislation/.

Private rights of action are not necessarily common in privacy laws and, in fact, have more than once been the sticking point in a proposed privacy bill's passage.[176] Businesses tend to see private rights of action as more of a potential "gotcha" and states have been leery of the vigorous industry pushback that often accompanies private rights of action in privacy bills. Proponents of private rights of action contend that the private rights of action can be tailored in such a way that they achieve the desired goals listed above but are sufficiently limited (for example, there can be huge variances in the level of harm or potential harm thresholds required to bring suit, how individuals can establish standing, types of personal data the private right of action may apply to, or types of violations that may be applicable).[177]

Considering both the concerns of businesses and the benefits that a private right of action would provide to individuals and enforcement agencies, we feel that private rights of action are a meaningful addition to bills addressing privacy issues in XR technologies and should be considered and incorporated where possible. When compared with industry-based self-regulatory approaches, legislation is the more effective and consistent approach to ensuring privacy protections in XR technology, particularly in the private sector. But to ensure limits on law enforcement or government overreach, there should also be continued movement towards privacy protections in the judiciary.

2. Judicial

As we've already discussed, courts are currently using a mix of Fourth Amendment approaches to analyze both the law enforcement collection of data from third parties and law enforcement direct search and surveillance. It is possible that the courts will be able to create a path forward for either of these two areas by using the framework that the Supreme Court has created in *Carpenter*. However, there are several potential problems with this approach.

Judicial action is unlikely to apply to private sector risks in XR due to the lack of a private right of action in most privacy legislation. In

---

[176]*See* Aaron Nicodemus, *Private Right of Action Proving Problematic for State Privacy Laws,* COMPLIANCE WEEK (May 5, 2021), https://www.complianceweek.com/data-privacy/private-right-of-action-proving-problematic-for-state-privacy-laws/30343.article.

[177]*See supra* note 57; Cameron F. Kerry and John B. Morris Jr., *In Privacy Legislation, a Private Right of Action Is Not an All-Or-Nothing Proposition*, BROOKINGS (July 7, 2020), https://www.brookings.edu/blog/techtank/2020/07/07/in-privacy-legislation-a-private-right-of-action-is-not-an-all-or-nothing-proposition/.

addition to lack of private sector coverage, there are three typical weaknesses of common law which would apply to the Judicial approach. First, the length of time required to establish enough case law and precedent to create common law is incompatible with the speed at which new technology—including new methods of infringing on privacy rights—develops. XR technology is already in use and collecting personal data at breakneck speeds. In the time it may take to establish common law that would address the use of XR technology, it may have expanded and advanced even further, becoming enmeshed with day-to-day life and making disentanglement more challenging. In this case and others, while individual cases may be able to address specific problems more quickly than other methods, broad privacy common law would be forever playing catch-up to new violations.

Second, the nature of common law is reactive rather than proactive. It would be developed after violations have already occurred rather than proactively prevent violations. By the time privacy violations have occurred, it is highly unlikely the harm from the privacy violation can be undone, especially when it comes to sensitive information (e.g., biometrics). In the case of XR technology, we would need clear and arguable examples of violations combined with willingness to pursue judicial redress in order to begin establishing the necessary case law. Finally, common law can be overridden at any time by new legislation. The time and effort required to establish a common law privacy protection could be instantly undermined by regulations and may not be considered stable.

While many look to the courts to provide clarity around existing protections, it is unlikely that courts can effectively develop protections through decision-making and, perhaps, inappropriate to look to the courts to set the tone on privacy protections in XR without guidance from legislators, technologists, and privacy specialists in the XR space.

3. XR Governance

There are several XR industry groups at this point in time, and there are bound to be many more as XR continues to take hold with the public.[178] At this point in time, there does not appear to be a framework

[178] Existing XR industry groups include the Extended Reality Association (XRA), a trade association; the XR Safety Initiative (XRSI), a non-profit focused on privacy, security, and ethics in XR across a broad set of industry sectors; the VR/AR Association, another trade association; and the EuroXR Association, a group focused on XR (AR/VR/MR) in Europe.

for XR development that is used across the industry. XRSI has recently put forth a XR Privacy Framework that maps controls to general categories of privacy in an effort to aid XR developers with privacy by design.[179] While this is a strong first step, without widespread adoption and conversation around the framework, it is unlikely that an industry standard for XR governance will appear. It is critical that the industry move towards published standards for XR to help protect XR technology *and* mitigate or prevent harms. We note, however, that industry standards are not a substitute for regulatory limitations and fall prey to several pitfalls in enforcement and stability.

CONCLUSION

Despite the proliferation of development in XR technology, the existing U.S. privacy framework addressing it remains weak, both in the private and public sectors. Throughout this paper, we have detailed possible scenarios of privacy harms. We recommended solutions that legislators can embrace to protect privacy as it currently exists and even enhance individual privacy rights and protections. XR technology is moving quickly and our legislators must work with technical specialists and privacy advocates to match the speed. Even as we write our assessments of the dangers of XR without strong regulations, we see that XR technology has moved from specialized gaming and industrial/corporate uses into technology that is available to the masses through existing social media giants. We urge legislators to address the gaps we have identified before XR technology further embeds itself into the fabric of our lives.

[179] THE XRSI PRIVACY AND SAFETY FRAMEWORK, XR SAFETY INITIATIVE (Kelly J. Cooper, ed., v 1.0, 2020) (We provided high-level review of the privacy framework during early-stage development. We are not affiliated with or employed by XRSI).