Virtual Reality and Students: The Privacy Issues Are Still Real

> "Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing… Unauthorized disclosure, use, and dissemination of personal information regarding minors."
> (FCC, "Children's Internet Protection Act")

Imagine an American teacher introducing her students to Arundhati Roy's novel *The God of Small Things*, which is set in the Indian state of Kerala. She might be worried that some of her students (those who didn't grow up in India, at least) will have a difficult time imagining the novel's world. Though Roy is skilled at evoking a vibrant atmosphere of rivers, villages, and families in her writing, the environment might be so different for some American students that they won't be able to connect with the story.

Now also imagine this teacher has several virtual reality (VR) systems in her classroom. For the purposes of this paper, "virtual reality" will be defined as technology that manipulates the sensory stimuli of users so they feel as if their bodies were in different locations than their actual physical bodies. Just a few examples of VR technology might include: 1) a visor and earphones that users put on their heads to provide visual and auditory stimuli; 2) a machine that users climb inside, which then imitates the movements of a vehicle (like a flight simulator); 3) a computer in the (maybe not distant) future that directly stimulates users' brains to create neural signals. (VR is distinguished from "augmented reality" or "mixed reality," which add virtual objects to users' perceptions of the environments around their actual physical bodies. However, the privacy issues discussed in this paper also mostly apply to augmented reality and mixed reality.)

When our teacher has her students put on the VR headsets, their 360° fields of vision are completely filled with a Kerala village. The students can walk through a bustling market, lean forward to closely examine mounds of local fruit, lift their eyes to the sky, and turn their heads to follow the movement of people walking past. Through the earphones, they can hear birds singing

and conversations between shoppers and merchants. When they take off the headsets, they now have direct sensory memories that they can use to construct Roy's environment in their minds. Their imaginations will still have to work hard to flesh out the novel, but they now have some basic building blocks to help them.

This might seem like science fiction to some readers, but it is largely possible today with a variety of VR systems for sale to the general public at relatively affordable prices. The Oculus Go, for example, sells for around $179 and doesn't require a dedicated computer or smartphone (Best Buy website). Around 20 million VR systems were bought by consumers in 2017 from companies such as Oculus (which is owned by Facebook), HTC, Sony, Samsung, and Google (Wall, Matthew). Although the visual quality of these systems is still far from the crispness of most modern two-dimensional monitors, it is likely only a matter of time until VR catches up with two-dimensional visual quality. As the data visualist Lev Manovich has written: "…as the processing power and RAM size keep increasing, these differences between the graphics capacities of various hardware platforms and software are gradually disappearing" (Manovich 22). In addition, the current level of visual quality can be compensated by the powerful sensation of "presence" that comes from VR's three-dimensional stimuli.

The above classroom scenario shows how tempting it could be for some teachers to use this new VR technology with their students. The anthropologist Brian Larkin has written that infrastructure can "encode the dreams of individuals and societies" (Larkin 333), and at times, VR can seem like a spectacular realization of that ideal. However, it is essential for teachers to remember that while their students are observing the wonders of the virtual worlds around them, they are also being observed. Everything that VR users see and hear in a virtual environment, every movement that they make, biometric data like the contours of their bodies, and other

personal aspects are constantly (and I am literal when I use the word "constantly") being collected and analyzed by the VR technology.

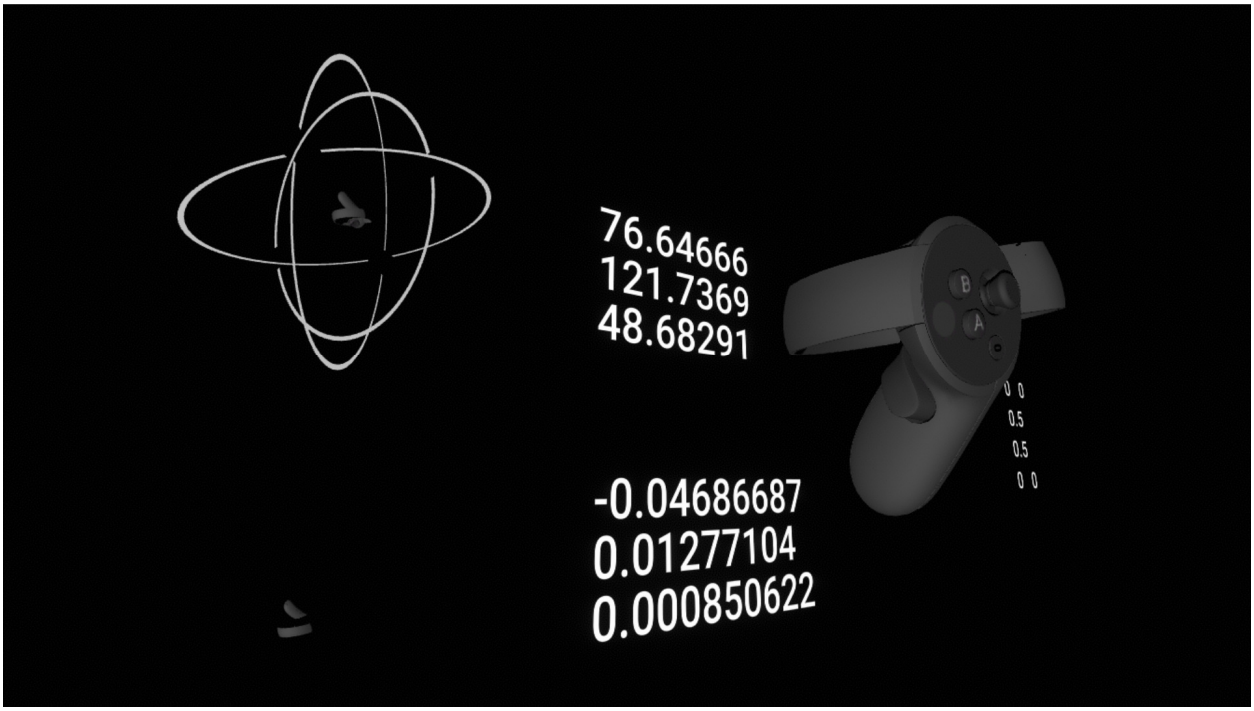
An understandable reaction to that last sentence is indignation. Teachers might insist that VR technology simply not ubiquitously surveil their students. Unfortunately, this is one of the conundrums of VR. The nature of the technology is such that extreme tracking of users' bodies is necessary for it to properly function. Jeremy Bailenson, the founder of the Virtual Human Interaction Lab, has written about his lab's experiments:

> In order to create presence, three technical elements have to be executed flawlessly: tracking, rendering, and display… If any one of these elements is off, users can experience simulator sickness… We looked at a dozen features, ranging from image-resolution to display field of view to sound quality. Tracking was at the top of the list… At talks, when describing virtual reality technology, I often tell a joke. What are the five most important aspects of VR technology? The punch line: Tracking, Tracking, Tracking, Tracking, and Tracking. (Bailenson 22)

If a VR system didn't track a user's motion or body contours, it would not know where a user was standing in the virtual environment, which direction the user's head was facing, or where the limbs of the user were in relation to his body. These are necessary for good "rendering," which is the adjustment of sensory stimuli during a VR experience. Good rendering allows virtual objects to be viewed from different angles and smoothly change size as the user moves toward or away. Bad rendering makes virtual objects stutter and jump as the user's perspective changes. (It can also cause the aforementioned simulator sickness, which is basically the same as the motion sickness you might feel on a boat.) If tracking were removed completely, VR would be no different than watching a two-dimensional screen.

To give an appreciation of how finely a VR system tracks its users' movements, below is a screenshot from a VR experience called *Virtual Virtual Reality* (Tender Claws). This is from a section of the experience where users can watch the VR system track their movements in real

time. The unit of measurement is not specified, but considering that it is being monitored to as much as the ninth decimal place, the tracking appears to be extremely fine indeed.



As you can see, virtual environments are surveillance environments almost by definition.

The Children's Online Privacy Protection Act (COPPA) requires parental consent before a company collects any online information from children under 13 years of age (FCC website). The Children's Internet Protection Act (CIPA) requires schools to have an internet policy designed to protect the privacy of any minor who is under the age of 17 (ALA website). Considering the surveilling nature of VR technology and its connection to the internet, it seems reasonable to assume that COPPA and CIPA would require at a minimum that teachers have a policy for VR that parents can review and receive parental consent before letting students use VR. (Teachers also need to be aware of the potential social stigma or academic problems that might occur with students whose parents do not give them consent to use VR.) Depending on their location, additional consideration of minors' privacy rights might be required by

government regulations like CalOppa and GDPR.

Parental review and consent isn't enough, though. Such a small percentage of people are currently thinking about or using VR that the issue of virtual privacy is probably not on many parents' radar. Even optimistic data from the VR industry itself estimated that only about 3% of the American population used VR on a monthly basis in 2017 (Roettgers). The first VR Privacy Summit was held at Stanford University on November 8, 2018, but only about 50 people attended (Voices of VR 717). The Electronic Frontier Foundation, one of the most prominent non-profit advocates of internet privacy, has openly admitted that VR is not a major concern for it right now. In an interview, the EFF's David Maass said that the foundation's current battles in areas like free speech and libel have been consuming so much time that "if this had been three years ago, I would have said I'm going to run back and we're going to start hammering out white papers on VR… but I'm not sure that we're going to be able to jump on it as quickly we would have under other circumstances." However, Maass was also worried about waiting too long to get started on VR privacy issues: "I worry that what's going to happen is that we're going to have to deal with it reactively." (Voices of VR 714)

In addition, some parents who are aware of VR privacy issues might not care. There are some people who do not mind being heavily surveilled on the internet. Even after a variety of social media scandals, the Pew Research Center found in 2017 that "9% of social media users were 'very confident' that social media companies would protect their data" (Rainie). There are people who willingly put themselves on reality television shows where every waking (and sleeping) moment is filmed. There are people who openly and purposely keep detailed records of their health on public websites.

Thus, to a large extent, it might be up to teachers to act as the main line of defense

between their students and potential violators of their privacy. Parental consent might give teachers legal protection, but in order to safeguard their students beyond that, they might want to consider the following issues:

1. Biometric and health data – student bodies are being tracked

Considering that the only things touching a student's body in most VR systems are a visor and earphones, teachers might wonder how much biometric and health data the systems can really measure. An HTC Vive can't draw blood, take urine samples, or sequence DNA.

First, it should be noted that the inability of VR systems to make detailed physiological measurements is mostly a matter of the current state of the technology, not an inherent quality. Haptic (engaging the sense of touch) full-body suits have been part of experimental VR for several years. The major barrier to their sale to consumers now is probably cost, but prices will likely fall as manufacturing is scaled up. A suit in contact with most of a user's outer surface could probably relatively easily collect many of the physiological measurements that doctors currently do. There may come a day when users take off their haptic suits after a day of virtual work and receive an alert that their calcium level is low.

However, even without full-body suits, there is a wide variety of bodily information that current VR systems can gather about users. One of the first questions that a VR system asks a user is her height, in order to configure the area of user motion. The speed with which users react to sights and sounds can measure vision and hearing abilities. Particular movements might tend to be associated with disabilities such as cerebral palsy or attention-deficit disorder.

The philosopher Thomas Metzinger has detailed many of the possible commercial uses of recording patterns of movement in his "Code of Ethical Conduct for VR":

> Commercial applications of virtual environments introduce new possibilities for targeted advertising or "neuromarketing," thus attacking the individual's mental

> autonomy. By tracking the details of one's movements in VR, including eye movements, involuntary facial gestures, and other indicators of what researchers call low-level intentions or "motor intentions," private agencies will be able to acquire details about one's interests and preferences in completely new ways. If avatars themselves should in the future be used as "humanoid interfaces," consumers can be influenced and manipulated by real-time feedback of the avatar's own facial and eye movements (for example, via automatic and unconscious responses in their mirror-neuron system). Commercials in VR could even feature images of the target audience himself or herself using the product. The use of big data to "nudge" users ("Big Nudging") combined with VR could have long-lasting effects, perhaps producing changes in users' mental mechanisms themselves. (Metzinger)

Some American teachers might understandably think that VR companies are restricted from collecting or selling users' biometric and health data because of the United States' Health Insurance Portability and Accountability Act (HIPAA), which regulates how medical information can be collected and used by a variety of health care providers. However, the American Bar Association has warned its members that HIPAA only covers a relatively narrow range of entities:

> The rules that implement these laws apply to health plans, health care clearinghouses, and healthcare providers, collectively referred to as "Covered Entities" working with protected health information (PHI)—individually identifiable health information that a Covered Entity creates or receives.
>
> Wearable device manufacturers are not ordinarily exposed to HIPAA liability, because they are not Covered Entities, and their products and services work directly with the consumer, keeping Covered Entities out of the loop. (ABA website)

If wearable technology (like the popular fitness-tracking devices FitBit and Garmin) are not covered by HIPAA, despite collecting physical data on users like heart rate and sleep patterns, it is difficult to see how VR systems would be treated differently under the law.

Internet child-protection laws like COPPA and CIPA probably override much of the "third-party doctrine" in regards to online privacy, as long as companies are reasonably aware that they are interacting with minors. The third-party doctrine is a legal precedent repeatedly

upheld by the U.S. Supreme Court which maintains that if people voluntarily give information to a third party, they can have no reasonable expectation that it will be kept private (Supreme Court). Despite COPPA and CIPA, though, the lack of protections for adults due to the third-party doctrine make it that much easier for children to slip through the cracks.

2. Social and psychological lives can be tracked too

People's movements are not just potential indicators of medical conditions – they are also potential indicators of opinions, beliefs, and desires. By monitoring what students do in a virtual environment, it might be possible to make assumptions about their political leanings. In a virtual environment completely constructed by computers, police with access to those computers could track who students talk with or what types of organizations they belong to. Authoritarian governments could monitor student behavior that they consider threatening, even if the students' physical bodies are in countries with strong free speech protections. This last point highlights the privacy considerations that American teachers must be aware of with students who are citizens of other countries.

In addition, the more flexible nature of children's minds can make them particularly susceptible to propaganda, both commercial and political. In one of his experiments on how children interpret VR experiences, Jeremy Bailenson noted that "after giving kids a VR experience of swimming with whales, many formed 'false memories,' believing they had actually physically been to Sea World to see an Orca." (Bailenson 72) In another experiment with children and VR, the children showed a far greater willingness to imitate a Sesame Street character in VR than when only watching the character on television (Bailey).

The pioneering VR engineer Jaron Lanier has written about himself and his fellow programmers: "We tinker with your philosophy by direct manipulation of your cognitive

experience… It takes only a tiny group of engineers to create technology that can shape the entire future of human experience with incredible speed." (Lanier 6)

3. Corporate control of VR – your data is being collected

COPPA does not allow internet companies to collect data about children under the age of 13. However, unless they are made reasonably aware that children under 13 are using their services, COPPA "does not require operators of general audience sites to investigate the ages of visitors to their sites or services." (FCC website) In addition, COPPA does not apply to children 13 years old or above. CIPA applies to children under 17 years of age, but only states that schools need to have a policy about protecting the privacy of minors, not that companies need to protect that privacy: "Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing… Unauthorized disclosure, use, and dissemination of personal information regarding minors." (FCC website) Therefore, a lot of loopholes exist for children's data to fall into corporate hands.

Over the past few years, there seems to have been a public awakening about how much data is being collected and sold by the companies that own popular websites and smartphone apps. Governments around the world have held high-profile hearings on consumer privacy featuring Mark Zuckerberg, the CEO of Facebook, and Sundar Pichai, the CEO of Google. Cambridge Analytica, a data analysis company, collected data on more than 50 million Facebook users (most of whom did not give permission), and sold that data to political and corporate entities (Ingram). In December 2018, the *New York Times* reported on a variety of smartphone apps that collected data on users without their explicit knowledge and how that data could easily be used to identify a particular user, potentially revealing what types of doctors they were visiting or which churches they were attending (Valentino-DeVries). If this much data can be

collected from simply keeping track of a smartphone as its user travels through particular roads or buildings, imagine how much more can be collected when the roads, buildings, and everything else in a virtual environment are built and maintained by computer software.

Although there is an extensive array of non-profit VR experiences, and a growing body of non-profit VR software, high-quality affordable VR hardware systems are only currently available through for-profit companies like Sony and Samsung. Although there is an affordable VR hardware system which calls itself "Open Source Virtual Reality" (OSVR), deeper probing of its website reveals that the system is actually made by the computer and gaming company Razer, which is very much for-profit.

Of course, just because hardware is made by a privately-owned company doesn't necessarily mean that the hardware is collecting significant data on users. There have not been many incidents (at least public ones) of computer manufacturers compromising user privacy – but it is not unprecedented. In 2014, for example, Lenovo preinstalled its computers with software that not only tracked users' websites in order to insert ads, but also inadvertently allowed hackers to impersonate trusted websites (Goodin). Automobile manufacturers have preinstalled their vehicle computers with software that tracks the locations of drivers (Quain).

However, while most computer manufacturers use operating systems that were developed by other companies (like Microsoft Windows), VR companies like Oculus and Sony create both the hardware and operational software of their VR systems. When a user puts on the headset of an Oculus Rift VR system, the default virtual location is Oculus Home, where the user can virtually select and buy experiences or adjust the system's settings.

Due to privacy regulations in the European Union, Oculus allows users to download some of the information that it collects about them. I downloaded my own Oculus data as part of

this research paper. It included every VR experience that I had ever downloaded through the Oculus Home library and store, the time that I had downloaded them, and a seemingly random assortment of my logins. Fortunately, there didn't seem to be any biometric data, but I question how many users would notice if it began appearing there.

4. Different companies have different privacy policies

When a VR system is working well, the underlying software and hardware feel like they have disappeared. In the moment, it might be difficult to remember whether your head is clad in a Gear VR system made by Samsung or a Vive made by HTC. However, each separate VR company has a separate privacy policy and there can be significant differences among them. There is not enough space in this paper to cover the hundreds of small start-up companies that have begun making VR experiences, so I will focus on a few differences among the major VR system makers.

For example, HTC often refers to the "rights" of users (HTC website), but Oculus never refers to "rights" at all (Oculus website). Sony refers to "rights," but almost only in reference to the company's rights (Sony website). In addition, Sony refers to the "Swiss-U.S. and E.U.-U.S. Privacy Shield," but Oculus and HTC do not. Of course, the lack of mentioning these items does not indicate that the companies will not follow them, but it might indicate the sense of focus within the companies.

The major takeaway is that teachers should read the privacy policy of any VR system before letting their students use it, and not assume that it will be the same as other VR systems. Teachers should also be aware that most VR systems explicitly state in their warnings that children under 13 years of age should not use them.

5. Private individuals can watch students too

With all the news reports about companies collecting personal data, it can be easy to forget that private individuals spy on each other too. For example, I was not even aware of my first engagement with the larger Oculus social network of users. I had been experimenting with a game called *Dead and Buried*, thinking the entire time that the other characters were computer-generated. It was only after the game ended that I learned the other characters were being controlled by humans in other locations. Although there was a humorous aspect to this (since I had acted far more "annoyingly" than I would have if I had known), it was also disturbing to realize that I hadn't been able to tell that the characters were human simply from their behavior.

I'm not alone in this difficulty, though. There have been several experiments showing the difficulty that people can have in telling humans from artificial intelligence, such as the Eliza experiment from the 1960s (Garber) and the more recent Google Duplex software that could make reservations with human receptionists over the phone (Simonite). Most people seem to have worried about this issue from the perspective of artificial intelligence impersonating humans so well that people lose their willingness to socially engage with actual human beings. From a privacy perspective, however, the reverse seems true. If it becomes almost impossible for people to tell the difference between real and computer-generated characters, it could be easy for humans with less-than-pure motives to slip in among benign computer-generated children's characters without the awareness of supervising adults.

6. User experiences are subjective and can be difficult to supervise

When using a two-dimensional computer or mobile screens, advertisements are usually fairly noticeable, because it can be difficult for them to fit smoothly into the construction of a particular website or app. Although children can be very skilled at hiding forbidden activities from adults, if a student happens to find a website on a classroom computer that a teacher finds

unacceptable, it is still relatively easy for that teacher to spot this by simply looking at the student's screen.

However, when a student puts on a VR headset, her particular VR experience is only fully seen from her subjective point of view. It thus becomes far more difficult to supervise what she is seeing. The perspective from the headset is usually also displayed on the computer screen to which the VR system is attached, but the two-dimensional screen view is distorted because the images are built for three-dimensional schematics. Plus, the screen view is so small compared to the 360° world that the user is inhabiting. In the VR environment, a toothpaste box looks the same size as a toothpaste box in the physical world, but on the attached two-dimensional screen that a teacher would supervise, it would barely be a dash.

Imagine a student walking down a virtual street in VR. In that environment, it would be very natural to have advertising billboards or posters in the windows of shops. If the student entered a virtual grocery store, it would be natural to have various branded products on the shelves. These are just a couple ways that ads can easily fit into a VR experience. Perhaps a child's movements have followed a pattern of behavior that complex algorithms have determined tend to lead to buying a particular brand of candy or pharmaceutical. Or maybe there will be a glitch in the algorithms and child safeguards won't be in place, leading to ads for liquor or pornography. Only the user of a particular VR system can fully know what is being seen in his VR environment, so these features will likely go unnoticed by supervising adults.

Policies Moving Forward

To be clear, the privacy concerns stated above should not keep teachers from using VR with their students, since the benefits of VR use could potentially be tremendous. They are simply intended as areas of concern. However, teachers might want to put pressure on VR

companies to resolve some of these issues sooner rather than later. As political researcher Virginia Eubanks has noted: "Once they scale up, digital systems can be remarkably hard to decommission." (Eubanks 186) Faced with this assortment of privacy issues that seem necessary to address, what are some of the possible solutions? Here are just a few:

1. Don't store unneeded data

Currently, the privacy policies of many VR companies are very open-ended. For example, Sony merely states that it might automatically collect "physical or geographic location data" (Sony website). HTC says "We may collect information about your usage of and activity on our Services." (HTC website) Although the difficulty in using or recording biometric data is still too high to be much threat to users, these nebulous wordings seem tailor-made for future privacy violations as biometric data collection becomes more efficient and effective.

In response to journalist questions about Oculus's vague biometric privacy statements, company representative Max Cohen offered the example of how a user's height is only stored in the user's personal system, not on the servers at Oculus. Cohen also claimed that the company intends to act similarly as other biometric data become significant in the functioning of Oculus's VR systems (Voices of VR 641).

Many VR companies are aware of the legal issues surrounding minors and VR. (Though this might be more from fear of legal liability than from genuine concern for children.) Most VR systems explicitly state that children under 13 years of age should not use their systems at all, in addition to stating that they will not collect data on minors. If teachers have concerns about data that might have been collected about their students, they should at least contact the VR company responsible and/or the maker of the VR system.

2. Anonymize data

Whenever possible, VR companies of all kinds, no matter how large or small, should strip collected data of any markers that associate it with individual users. The larger VR companies, most being offshoots of well-established technology companies, already make at least some attempt to do this. Jenny Hall, the lead privacy policy architect at Oculus, has said: "We don't tie this [biometric data] to personal identity. When information is transmitted to our servers, we divorce that from any kind of identifying information. So we may know that 500 people have a certain play space, but we don't know that [name of coworker]'s space is two and half feet." (Voices of VR 714) However, as more VR start-ups emerge, they will sometimes be unaware of the need to anonymize data. Teachers should be aware of this when using VR from new or small companies.

However, even with large established VR companies, it is difficult to truly anonymize data. Journalists have been able to piece together personal identities fairly quickly with supposedly anonymized public data collected by internet companies (Singer). Unfortunately, "anonymization" is a term without rigorous standards, and whether or not data is truly anonymized is at the discretion of the company collecting the data.

3. Awareness

Parents need to know very clearly what they are signing their children up for. Thomas Metzinger writes: "Users ought to be made aware that there is evidence that advertising tactics using embodiment technology such as VR can have a powerful unconscious influence on behavior." (Metzinger website) CIPA requires that schools create internet policies and allow parents to access those policies. This should likely also be the case for virtual reality. In addition, teachers might want to personally discuss virtual reality privacy issues with parents.

In this paper's Appendix, I have included a potential prototype of a VR parental consent

form that teachers might use as a basis for creating their own consent forms. It is based on various parental consent forms for internet use already employed by some schools and libraries. However, this form is only a prototype and needs to be reviewed by a school's lawyer before being used with actual students.

4. Opting in

Journalist Kent Bye, who has reported extensively on VR privacy issues, has emphasized that VR companies should have users "opt in" rather than "opt out" of privacy rules (Voices of VR 717). This is especially true considering how many variables might be involved in future VR experiences. In the same way that many websites are no longer simply controlled by the owner of the URL, but instead are pastiches of code from a variety of sources, 360° VR environments will someday be filled with different developer programs. Today, if you enter a VR city, the entire city has almost assuredly been designed and maintained by a single company. In the future, it is easy to imagine each store built by a different company. When you enter a particular store, you would suddenly be in that company's environment and perhaps subject to a new privacy policy. At this point, it seems undecided who would be considered responsible for the store's exterior. I predict there will eventually be VR legal battles similar to those we have seen over the responsibility of property owners in the physical world.

5. Open-source VR systems

To better protect student privacy, it would be helpful if the hardware for VR were not completely dominated by large corporate entities. There are currently non-corporate cardboard headsets available, but they rely on smartphones to provide content, and smartphones are corporately produced and operated. Teachers should encourage the development of VR hardware that is truly open-source (as opposed to Razer Incorporated's "Open Source Virtual Reality").

Open-source friendly technologies like 3D printing and Arduino might eventually produce viable open-source VR hardware, and teachers should probably encourage that development.

Conclusion

Concerns about the privacy of students in VR are very real. Because VR privacy is still not an issue for almost anyone (never mind children), it is probably necessary for teachers to be the primary line of privacy defense when using VR with students. Even after receiving parental consent for students to use VR, there are so many potential areas of privacy violation that teachers have to be vigilant when supervising their students.

However, I would like to end on an optimistic note. Reasonable worries about privacy should not keep teachers from using VR systems with their students. Teachers should not forget that VR has tremendous potential to foster empathy and learning. As just a few examples, the Anne Frank House has created a free virtual tour that allows students to see what the annex looked like when the Frank family lived there. The *New York Times* offers 360° VR videos allowing students to explore the ocean beneath the Antarctic ice cap or to walk through a Syrian refugee camp. Students at the 2018 XR Brain Jam created a VR experience from the perspective of a lab animal trying to figure out an experiment, in order to create empathy for the animal's point of view. As Jaron Lanier has written:

> There is something extraordinary that you might care to notice when you are in VR, though nothing compels you to: you are no longer aware of your physical body. Your brain has accepted the avatar as your body… any part of reality might just as well be a part of your body if you happen to hook up the software elements so that your brain can control it easily. Maybe if you wiggle your toes, the clouds in the sky will wiggle too. Then the clouds would start to feel like part of your body. All the items of experience become more fungible than in the physical world. *And this leads to the revelatory experience.* [emphasis added] (Lanier 187)

As much as any technology in history, VR has the potential to make the world a better place. Teachers should not be afraid to use it – just be careful.

Appendix

The following is a potential PROTOTYPE parental consent form for students to use VR in the classroom. It is based on various parental consent forms already used by some schools and libraries. Please be advised that this is NOT a lawyer-reviewed legal document. Teachers should have this form reviewed by their school's lawyers and make appropriate modifications before using it with students.

Student Permission Form for Virtual Reality Use

As the parent or legal guardian of _____, I grant permission for my minor child to use virtual reality at [name of school]. I have read the school's virtual reality policy and discussed it with my child or children. I understand that some privacy risks and/or objectionable material might be encountered in a virtual environment.

I further hold [name of school] harmless from any damages caused by my child's or children's use of virtual reality. This includes physical damage caused while using virtual reality equipment, virtual damage caused to virtual objects or people within the virtual reality environment, and/or emotional / psychological / reputational damage caused within the virtual reality environment.

Signature of Minor _____

Signature of Parent or Guardian_____

Date_____

Works Cited

ABA (American Bar Association). "Regulating Wearable Devices in the Healthcare Sector." 27 Sep. 2018. https://www.americanbar.org/groups/health_law/publications/aba_health_esource/2014-2015/may/devices/. Accessed 9 Dec. 2018.

ALA (American Library Association). "CIPA Legal FAQ." http://www.ala.org/advocacy/advleg/federallegislation/cipa/cipalegalfaq#minor. Accessed 12 Dec. 2018.

Bailenson, Jeremy. *Experience on Demand.* W.W. Norton & Co., 2018.

Bailey, J.O. et al. "Virtually True: Children's Acquisition of False Memories in Virtual Reality." *Media Psychology,* no. 12, 2009.

Best Buy. "Oculus Go - 32GB Stand-Alone Virtual Reality Headset." https://www.bestbuy.com/site/oculus-go-32gb-stand-alone-virtual-reality-headset/6212949.p?skuId=6212949&ref=212&loc=1&ds_rl=1260672&ds_rl=1266837&ref=212&loc=1&gclid=EAIaIQobChMI2uv07qqi3wIViInICh2tkga9EAYYAyABEgI7bfD_BwE&gclsrc=aw.ds. Accessed 16 Dec. 2018.

Eubanks, Virginia. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press, 2018.

FCC (Federal Communications Commission). *Children's Internet Protection Act (CIPA).* 8 Sep. 2017. https://www.fcc.gov/consumers/guides/childrens-internet-protection-act. Accessed 10 Dec. 2018.

FCC (Federal Communications Commission). *Complying With COPPA: Frequently Asked Questions.* 20 Mar. 2015. https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions. Accessed 10 Dec. 2018.

Garber, Megan. "When PARRY Met ELIZA: A Ridiculous Chatbot Conversation From 1972."

The Atlantic. 9 June 2014. https://www.theatlantic.com/technology/archive/2014/06/when-parry-met-eliza-a-ridiculous-chatbot-conversation-from-1972/372428/. Accessed 14 Dec. 2018.

Goodin, Dan. "Lenovo PCs ship with man-in-the-middle adware that breaks HTTPS connections." *Ars Technica.* 19 Feb. 2015. https://arstechnica.com/information-technology/2015/02/lenovo-pcs-ship-with-man-in-the-middle-adware-that-breaks-https-connections/. Accessed 17 Dec. 2018.

HTC. "Privacy Policy." 25 May 2018. https://www.htc.com/us/terms/privacy/. Accessed 28 Nov. 2018.

Ingram, David. "Factbox: Who is Cambridge Analytica and What Did It Do?" *Reuters.* 19 Mar. 2018. https://www.reuters.com/article/us-facebook-cambridge-analytica-factbox/factbox-who-is-cambridge-analytica-and-what-did-it-do-idUSKBN1GW07F. Accessed 13 Dec. 2018.

Lanier, Jaron. *You Are Not a Gadget.* Vintage Books, 2011.

Larkin, Brian. "The Politics and Poetics of Infrastructure." *Annual Review of Anthropology*, vol. 42, 2013.

Manovich, Lev. "What Is Data Visualization?" Oct. 2010. http://manovich.net/content/04-projects/064-what-is-visualization/61_article_2010.pdf. Accessed 3 Dec. 2018.

Metzinger, Thomas. "Real Virtuality: A Code of Ethical Conduct." *Frontiers in Robotics and AI.* 19 Feb. 2016. https://www.frontiersin.org/articles/10.3389/frobt.2016.00003/full. Accessed 2 Dec. 2018.

Oculus. "Oculus Privacy Policy." 4 Sep. 2018. https://www.oculus.com/legal/privacy-policy/. Accessed 28 Nov. 2018.

Quain, John. "Changes to OnStar's Privacy Terms Rile Some Users." *New York Times.* 22 Sep. 2011. https://wheels.blogs.nytimes.com/2011/09/22/changes-to-onstars-privacy-terms-rile-some-users/. Accessed 17 Dec. 2018.

Rainie, Lee. "Americans' complicated feelings about social media in an era of privacy concerns." *Pew Research Center.* 27 Mar. 2018. http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/. Accessed 15 Dec. 2018.

Roettgers, Janko. "Study Predicts Fewer Than 10 Million Monthly U.S. VR Headset Users This Year, 17 Million by 2019." Variety. 22 May 2017. https://variety.com/2017/digital/news/vr-headset-data-mau-2017-2019-1202440211/. Accessed 4 Dec. 2018.

Simonite, Tom. "Google's Human-Sounding Phone Bot Comes to the Pixel." *Wired.* 9 Oct. 2018. https://www.wired.com/story/google-duplex-pixel-smartphone/. Accessed 17 Dec. 2018.

Singer, Natasha. "With a Few Bits of Data, Researchers Identify 'Anonymous' People." *New York Times.* 29 Jan. 2015. https://bits.blogs.nytimes.com/2015/01/29/with-a-few-bits-of-data-researchers-identify-anonymous-people/. Accessed 15 Dec. 2018.

Sony. "Privacy Policy." 18 June 2018. https://www.playstation.com/en-us/network/legal/privacy-policy/. Accessed 28 Nov. 2018.

Supreme Court of the United States. "Smith v. Maryland." 20 June 1979. https://scholar.google.com/scholar_case?case=3033726127475530815. Accessed 11 De. 2018.

Tender Claws. *Virtual Virtual Reality.* 9 Mar. 2017.

Valentino-DeVries, Jennifer et al. "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret." *New York Times.* 10 Dec. 2018. https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html?mtrref=

www.google.com&gwh=72F0280F8058659A114ED578B8F0921E&gwt=pay. Accessed 11 Dec. 2108.

Voices of VR. "#641: Oculus' Privacy Architects on their Open-Ended Privacy Policy & Biometric Data." 19 Apr. 2018. http://voicesofvr.com/461-oculus-privacy-architects-on-their-open-ended-privay-policy-biometric-data/. Accessed 13 Dec. 2018.

Voices of VR. "#714: VR Privacy Summit: Electronic Frontier Foundation on Privacy on the Web." 20 Nov. 2018. http://voicesofvr.com/714-vr-privacy-summit-electronic-fontrier-foundation-on-privacy-on-the-web/. Accessed 12 Dec. 2018.

Voices of VR. "#717: VR Privacy Summit Organizer Highlights & Next Steps." 23 Nov. 2018. http://voicesofvr.com/718-vr-privacy-summit-organizer-highlights-next-steps/. Accessed 12 Dec. 2018.

Wall, Matthew. "Virtual reality as sharp as the human eye can see?" *BBC.* 23 Mar. 2018. https://www.bbc.com/news/business-42963408. Accessed 10 Dec. 2018.