Navigating Disruptive Technologies
Written Materials

American Bar Association
Section of Intellectual Property Law

2017 IP West

Navigating Disruptive Technologies
Internet Law & Policy Foundry

Panelists
Brian Focarino
Tiffany Li
Emory Roane
Gabriella Ziccarelli

Moderator
Natalie Nicol

October 11-12, 2017
Long Beach, CA
'New Rembrandt' to be unveiled in Amsterdam

Portrait is not a lost work by Dutch master but a 3D printed painting made by software that distilled the features of a Rembrandt

Mark Brown
Tuesday 5 April 2016 04.00 EDT

If people think the portrait of a 17th-century thirtysomething man in black hat and white collar looks unmistakably like a Rembrandt, then Bas Korsten will be a happy man. The painting's true creators are, however, data analysts and computers.

On Tuesday in Amsterdam, an artwork called “the Next Rembrandt” will be unveiled for the first time.

It is the result of an 18-month project which asks whether new technology and data can bring back to life one of the greatest, most innovative painters of all time.

Advertising executive Korsten, whose brainchild the project was, admitted that there were many doubters. “The idea was greeted with a lot of disbelief and scepticism,” he said. “Also coming up with the idea is one thing, bringing it to life is another.”

The project has involved data scientists, developers, engineers and art historians from organisations including Microsoft, Delft University of Technology, the Mauritshuis in The Hague and the Rembrandt House Museum in Amsterdam.

The final 3D printed painting consists of more than 148 million pixels and is based on 168,263 Rembrandt painting fragments.

Some of the challenges have been in designing a software system that could understand Rembrandt based on his use of geometry, composition and painting materials. A facial recognition algorithm was then used to identify and classify the most typical geometric patterns used to paint human features.

Korsten stressed the project was not trying to create a new Rembrandt. “We are creating something new from his work. Only Rembrandt could create a Rembrandt.”

There have been – and will be – critics of the project, said Korsten, people who object to having their idol messed with.

But many more “have embraced this as a way of getting to know more about Rembrandt and what made Rembrandt Rembrandt,” he said. “It is a way of keeping the great master alive.”

Many art historians, including the directors of the Mauritshuis and Rembrandt's house were on board and provided significant help.
The art historian Gary Schwartz called it “a fascinating exercise in connoisseurship”. He added: “The developers deserve credit for setting themselves to identify the features that make a Rembrandt a Rembrandt.

“While no one will claim that Rembrandt can be reduced to an algorithm, this technique offers an opportunity to test your own ideas about his paintings in concrete, visual form.”

Prof Joris Dik, who led the Delft University of Technology team, said: “There’s a lot of Rembrandt data available - you have this enormous amount of technical data from all these paintings from various collections. And can we actually create something out of it that looks like Rembrandt? That’s an appealing question.”

The idea was developed by the advertising agency J Walter Thompson in Amsterdam for its client, ING Bank. “They wanted us to match its innovation in the banking world in the domain of art and culture,” said Korsten, the agency’s executive creative director.

He hopes the project will be the start of a conversation about art and algorithms. “If you look at how music has embraced the computer, why doesn’t that happen in visual arts?

“It has taken some perseverance. There have been many moments when we’ve thought we’re not going to make it ... it’s too overwhelming, there’s too much information, too much data. But I think we have something decent to show people.”

• This article was amended on 5 April 2016. An earlier version said the painting would go on display at the Rembrandt House from 2 June. That is not the case.

Since you’re here ...

... we have a small favour to ask. More people are reading the Guardian than ever but advertising revenues across the media are falling fast. And unlike many news organisations, we haven’t put up a paywall - we want to keep our journalism as open as we can. So you can see why we need to ask for your help. The Guardian's independent, investigative journalism takes a lot of time, money and hard work to produce. But we do it because we believe our perspective matters - because it might well be your perspective, too.

I appreciate there not being a paywall: it is more democratic for the media to be available for all and not a commodity to be purchased by a few. I’m happy to make a contribution so others with less means still have access to information. Thomasine F-R.

If everyone who reads our reporting, who likes it, helps to support it, our future would be much more secure.

Become a supporter
Make a contribution

Topics
• Rembrandt
• Painting
• Art
Dallas Artist Chapman Kelley Takes Wildflower Case to Supreme Court

BY PETER SIMEK | PUBLISHED IN ARTS & ENTERTAINMENT | JULY 26, 2011 | 8:50 AM

Well, you knew this was coming. The latest on Dallas “wildflower artist” Chapman Kelley is that he has filed a petition with the Supreme Court requesting review of the decision of a Chicago court which denied the artist’s public art work in Grant Park protection under the Visual Artists Rights Act of 1990. If you are just tuning in, this long battle between the city of Chicago and Kelley, who lived in the city but has subsequently moved back to Dallas, began when the parks department altered his Chicago Wildflower Works, a landscape installation. Earlier this year, the 7th Circuit Court of Appeals ruled that Kelley had not sufficiently “authored” the piece to warrant protection under the Artists Rights Act. That law protects artists’ works from manipulation or destruction regardless of ownership.

There’s no word on whether or not the Supreme Court will accept Kelley’s case.

Here’s the release from Kelley’s advocate, John Viramontes:

Flawed 7th Circuit 2011 precedent in Visual Artists Rights Act case is ripe for U.S. Supreme Court review
U.S. arts community envision high court opening the door to protecting artists’ rights

On July 18, 2011, Dallas wildflower artist Chapman Kelley filed a petition with the Supreme Court of the United States requesting it to review the Seventh Circuit Court of Appeals (7th Circuit) February 2011 adverse decision to him in Kelley v Chicago Park District. The 7th Circuit had denied Kelley’s public artwork the Chicago Wildflower Works (CWW) protection under the Visual Artists Rights Act of 1990 or VARA saying that the work failed to hurdle two aspects of copyright law, namely, authorship and fixation.

*To our knowledge, never before in the history of U.S. copyright law has a professionally trained and exhibited artist such as Kelley had to defend a work of art against someone else’s definition of what constitutes art.*

In its February 2011 decision, the 7th Circuit’s “en banc” panel of justices, Daniel Manion, John Daniel Tinder and Diane S. Sykes unanimously said that Kelley had not “authored” CWW and that its flowers were not sufficiently “fixed” to merit protection under federal copyright law. During the same time period, this original panel of justices denied the timely filing of a amicus curiae – friend of the court brief – prepared in support of Kelley by the laudable Volunteer Lawyers for the Arts – New York.

The 7th Circuit’s decision about the true “author” of CWW leads one to believe that all those wildflower plant seeds, independently and collectively, created CWW. The time, money and effort expended on CWW was the seeds’ own making, instead of Kelley. What a preposterous idea! The justice’s notion of the lack of “fixity” of CWW, they ruled that flowers are “temporary” and therefore unable to be experienced or recorded in a meaningful way is just as contestable. The DNA of plants is so dependably fixed that
plants furnish us obviously with much of our food, clothing and shelter material.

After flourishing in a Chicago lakeside park for 20 years, during the summer of 2004 the Chicago Park District destroyed Kelley’s public artwork, the CWW. CWW was installed by him in 1984 as a noncommissioned work with official park district approval. At 66,000 sq. ft. its elements were organic and inorganic; many species of native Illinois plants configured in a double ellipse, framed in gravel and steel banding. CWW thrived solely on rainwater and used no insecticides or fertilizers. It was maintained for 20 years by an army of volunteers under Kelley’s direct supervision. It garnered wide acclaim and was an environmental success story ahead of its time. Notable about CWW was that it bloomed sequentially, constantly, through three seasons. Imagine the environmental and monetary savings.

Artists whose work has been altered without their permission have the federal copyright statute, VARA, to potentially aid them in their fight for justice. We say potentially because obviously justices are reluctant to recognize Kelley’s declaration and intention that his Wildflower Works was a work of art; Kelley initially entertained the notion that flowers could be used in art, publicly, since the mid-1970s. The Council for Artists’ Rights is not a legal scholar but it appears that those in the legal community use a term to differentiate what artists say and intend versus what the court recognizes as final and settled; the word is dispositive. So although Kelley had consistently utilized flowers in his public artwork for nearly three decades, the court has stripped him of his identity and considered his statements, action and intention as not dispositive and legally without merit.

Will the Supreme Court of the United States parrot the 7th Circuit’s adverse decision and carry on the tradition of being hostile to the arts community in the USA or will it instead
agree with Kelley’s (and other artists) decades-old declaration that flowers can be used in artwork?
Should the Supreme Court not take up the issue during it’s next term, when, if ever, will professional artists such as Kelley be allowed to control the material, image and therefore content of their creations, to call it art and have it protected by VARA?
If a court’s approval is going to be necessary for an artist’s choice of material and image, as implied by the 7th Circuit’s holding, then it is the court who controls content. Having the power to do so is a flagrant violation of all artists’ 1st Amendment right to free speech.
*Image: via.*
Chapman KELLEY, Plaintiff-Appellant/Cross-Appellee,

v.

CHICAGO PARK DISTRICT, Defendant-Appellee/Cross-Appellant.

Nos. 08-3701, 08-3712.

United States Court of Appeals, Seventh Circuit.

Argued September 10, 2009.

Decided February 15, 2011.

Rehearing and Rehearing En Banc Denied April 19, 2011.

United States Court of Appeals, Seventh Circuit.

Before MANION, SYKES, and TINDER, Circuit Judges.

SYKES, Circuit Judge.

Chapman Kelley is a nationally recognized artist known for his representational paintings of landscapes and flowers — in particular, romantic floral and woodland interpretations set within ellipses. In 1984 he received permission from the Chicago Park District to install an ambitious wildflower display at the north end of Grant Park, a prominent public space in the heart of downtown Chicago. "Wildflower Works" was thereafter planted: two enormous elliptical flower beds, each nearly as big as a football field, featuring a variety of native wildflowers and edged with borders of gravel and steel.

Promoted as "living art," Wildflower Works received critical and popular acclaim, and for a while Kelley and a group of volunteers tended the vast garden, pruning and replanting as needed. But by 2004 Wildflower Works had deteriorated, and the City's goals for Grant Park had changed. So the Park District dramatically modified the garden, substantially reducing its size, reconfiguring the oval flower beds into rectangles, and changing some of the planting material.

Kelley sued the Park District for violating his "right of integrity" under the Visual Artists Rights Act of 1990 ("VARA"), 17 U.S.C. § 106A, and also for breach of contract. The contract claim is insubstantial; the main event here is the VARA claim, which is novel and tests the boundaries of copyright law. Congress enacted this statute to comply with the nation's obligations under the Berne Convention for the Protection of Literary and Artistic Works. VARA amended the Copyright Act, importing a limited version of the civil-law concept of the "moral rights of the artist" into our intellectual-property law. In brief, for certain types of visual art — paintings, drawings, prints, sculptures, and exhibition photographs — VARA confers upon the artist certain rights of attribution and integrity. The latter include the right of the artist to prevent, during his lifetime, any distortion or modification of his work that would be "prejudicial to his ... honor or reputation," and to recover for any such intentional distortion or modification undertaken without his consent. See 17 U.S.C. § 106A(a)(3)(A).

The district court held a bench trial and entered a split judgment. The court rejected Kelley's moral-rights claim for two reasons. First, the judge held that although Wildflower Works could be classified as both a painting and a sculpture and therefore a work of visual art under VARA, it lacked sufficient originality to be eligible for copyright, a foundational requirement in the statute. Second, following the First Circuit's decision in Phillips v. Pembroke Real Estate, Inc., 459 F.3d 128 (1st Cir.2006), the court concluded that site-specific art like Wildflower Works is categorically excluded from protection under VARA. The court then held for Kelley on the contract claim, but found his evidence of damages uncertain and entered a nominal award of $1. Both sides appealed.

We affirm in part and reverse in part. There is reason to doubt several of the district court's conclusions: that Wildflower Works is not copyrightable. The district court's treatment of the contract claim is another matter; the Park District is entitled to judgment on that claim as well.
I. Background

Kelley is a painter noted for his use of bold, elliptical outlines to surround scenes of landscapes and flowers. In the late-1970s and 1980s, he moved from the canvas to the soil and created a series of large outdoor wildflower displays that resembled his paintings. He planted the first in 1976 alongside a runway at the Dallas-Fort Worth International Airport and the second in 1982 outside the Dallas Museum of Natural History. The wildflower exhibit at the museum was temporary; the one at the airport just "gradually petered out."

In 1983 Kelley accepted an invitation from Chicago-based oil executive John Swearingen and his wife, Bonnie — collectors of Kelley's paintings — to come to Chicago to explore the possibility of creating a large outdoor wildflower display in the area. He scouted sites by land and by air and eventually settled on Grant Park, the city's showcase public space running along Lake Michigan in the center of downtown Chicago. This location suited Kelley's artistic, environmental, and educational mission; it also provided the best opportunity to reach a large audience. Kelley met with the Park District superintendent to present his proposal, and on June 19, 1984, the Park District Board of Commissioners granted him a permit to install a "permanent Wild Flower Floral Display" on a grassy area on top of the underground Monroe Street parking garage in Daley Bicentennial Plaza in Grant Park. Under the terms of the permit, Kelley was to install and maintain the exhibit at his own expense. The Park District reserved the right to terminate the installation by giving Kelley "a 90 day notice to remove the planting."

Kelley named the project "Chicago Wildflower Works I." The Park District issued a press release announcing that "a new form of 'living' art was coming to Grant Park — "giant ovals of multicolored wildflowers" created by Kelley, a painter and "pioneer in the use of natural materials" who "attracted national prominence for his efforts to incorporate the landscape in artistic creation." The announcement explained that "[o]nce the ovals mature, the results will be two breathtaking canvases of Kelley-designed color patterns."

In the late summer of 1984, Kelley began installing the two large-scale elliptical flower beds at the Grant Park site; they spanned 1.5 acres of parkland and were set within gravel and steel borders. A gravel walkway bisected one of the ovals, and each flower bed also accommodated several large, preexisting air vents that were flush with the planting surface, providing ventilation to the parking garage below. For planting material Kelley selected between 48 and 60 species of self-sustaining wildflowers native to the region. The species were selected for various aesthetic, environmental, and cultural reasons, but also to increase the likelihood that the garden could withstand Chicago's harsh winters and survive with minimal maintenance. Kelley designed the initial placement of the wildflowers so they would blossom sequentially, changing colors throughout the growing season and increasing in brightness towards the center of each ellipse. He purchased the initial planting material — between 200,000 and 300,000 wildflower plugs — at a cost of between $80,000 and $152,000. In September of 1984, a battery of volunteers planted the seedlings under Kelley’s direction.

When the wildflowers bloomed the following year, Wildflower Works was greeted with widespread acclaim. Chicago's mayor, the Illinois Senate, and the Illinois Chapter of the American Society of Landscape Artists issued commendations. People flocked to see the lovely display — marketed by the Park District as "living landscape art" — and admiring articles appeared in national newspapers. Wildflower Works was a hit. Here's a picture:

*294 For the next several years, Kelley's permit was renewed and he and his volunteers tended the impressive garden. They pruned and weeded and regularly planted new seeds, both to experiment with the garden's composition and to fill in where initial specimen had not flourished. Of course, the forces of nature — the varying bloom periods of the plants; their spread habits, compatibility, and life cycles; and the weather — produced constant change. Some wildflowers naturally did better than others. Some spread aggressively and encroached on neighboring plants. Some withered and died. Unwanted plants sprung up from seeds brought in by birds and the wind. Insects, rabbits, and weeds settled in, eventually taking a toll. Four years after Wildflower Works was planted, the Park District decided to discontinue the exhibit. On June 3, 1988, the District gave Kelley a 90-day notice of termination.

Kelley responded by suing the Park District in federal court, claiming the termination of his permit violated the First Amendment. The parties quickly settled; in exchange for dismissal of the suit, the Park District agreed to extend Kelley's permit for another year. On September 14, 1988, the Park District issued a "Temporary Permit" to Kelley and Chicago Wildflower Works, Inc., a nonprofit organization formed by his volunteers. This permit authorized them "to operate and maintain a two ellipse Wildflowers Garden Display ... at Daley Bicentennial Plaza in Grant Park" until September 1, 1989. The permit stipulated that Kelley "will have responsibility and control over matters relating to the aesthetic design and content of Wildflower Works I," and Wildflower Works, Inc. "shall maintain the Wildflower Works I at no cost to the Chicago Park District including, without limitation, weeding and
application of fertilizer." Although it did not contain a notice-of-termination provision, the permit did state that "[t]he planting material is the property of Mr. Chapman Kelley" and that Kelley "may remove the planting material" if the permit was not extended. Finally, the permit provided that "[t]his agreement does not create any proprietary interest for Chicago Wildflower Works, Inc., or Mr. Chapman Kelley in continuing to operate and maintain the Wildflower Garden Display after September 1, 1989."

The Park District formally extended this permit each succeeding year through 1994. After that point Kelley and his volunteers continued to cultivate Wildflower Works without a permit, and the Park District took no action, adverse or otherwise, regarding the garden's future. In March 2004 Kelley and Jonathan Dedmon, president of Wildflower Works, Inc., attended a luncheon to discuss the 20th anniversary of Wildflower Works. At the luncheon Dedmon asked Park District Commissioner Margaret Burroughs if Wildflower Works needed a new permit. Commissioner Burroughs responded, "You're still there, aren't you? That's all you need to do."

Three months later, on June 10, 2004, Park District officials met with Kelley and Dedmon to discuss problems relating to inadequate maintenance of the garden and forthcoming changes to Grant Park necessitated by the construction of the adjacent Millennium Park. The officials proposed reconfiguring Wildflower Works — decreasing its size from approximately 66,000 square feet to just under 30,000 square feet and remaking its elliptical flower beds into rectangles. The District's director of development invited Kelley's views on this proposal but made it clear that the District planned to go forward with the reconfiguration with or without Kelley's approval. Kelley objected to the proposed changes, but did not request an opportunity to remove his planting material before the reconfiguration took place. A week later the Park District proceeded with its plan and reduced Wildflower Works to less than half its original size. The elliptical borders became rectilinear, weeds were removed, surviving wildflowers were replanted in the smaller-scale garden, and some new planting material was added. Dedmon sent a letter of protest to the Park District.

Kelley then sued the Park District for violating his moral rights under VARA. He claimed that Wildflower Works was both a painting and a sculpture and therefore a "work of visual art" under VARA, and that the Park District's reconfiguration of it was an intentional "distortion, mutilation, or other modification" of his work and was "prejudicial to his ... honor or reputation." See 17 U.S.C. § 106A(a)(3)(A). He also alleged breach of contract; he claimed that Commissioner Burroughs's remark created an implied contract that the Park District had breached when it altered Wildflower Works without providing reasonable notice. On the VARA claim Kelley sought compensation for the moral-rights violation, statutory damages, and attorney's fees; on the contract claim he sought the fair-market value of the planting material removed in the reconfiguration. He later quantified his damages, estimating the value of the plants at $1.5 million and requesting a staggering $25 million for the VARA violation.

The case proceeded to a bench trial, and the district court entered judgment for the Park District on the VARA claim and for Kelley on the contract claim. See Kelley v. Chi. Park Dist., No. 04 C 07715, 2008 WL 4449886 (N.D.Ill. Sept. 29, 2008). The judge first concluded that Wildflower Works could be classified as both a painting and a sculpture and therefore qualified as a work of visual art under VARA. Id. at *4-5. But he also held that Wildflower Works was insufficiently original for copyright, a prerequisite to moral-rights protection under VARA. Id. at *6. Alternatively, the judge concluded that Wildflower Works was site-specific art, and following the First Circuit's decision in Phillips, held that VARA did not apply to this category of art. Id. at *6-7. On the contract claim the court construed the Chicago Park District Act, 70 ILL. COMP. STAT. 1505/7.01, to permit individual commissioners to enter into binding contracts on the Park District's behalf. Id. at *7-8. The judge found that Commissioner Burroughs's statement — "You're still there, aren't you? That's all you need to do." — created an implied contract that the Park District had breached by failing to give Kelley reasonable notice before altering Wildflower Works. Id. But the judge also concluded that Kelley had failed to prove damages to a reasonable certainty and awarded $1 in nominal damages. Id. at *9.

Kelley appealed, challenging the adverse judgment on the VARA claim and the district court's treatment of the damages issue on the contract claim. The Park District cross-appealed from the judgment on the contract claim.

II. Discussion

This case comes to us from a judgment entered after a bench trial; we review the district court's factual findings for clear error and its conclusions of law de novo. Spurgin-Dienst v. United States, 359 F.3d 451, 453 (7th Cir.2004). In this circuit, questions of copyright eligibility *296 are issues of law subject to independent review. Schrock v. Learning Curve Int'l, Inc., 586 F.3d 513, 517 (7th Cir.2009).

1. A brief history of moral rights

That artists have certain "moral rights" in their work is a doctrine long recognized in civil-law countries but only recently imported into the United States. Moral rights are generally grouped into two categories: rights of attribution and rights of integrity. "Rights of attribution" generally include the artist's right to be recognized as the author of his work, to publish anonymously and pseudonymously, to prevent attribution of his name to works he did not create, and to prevent his work from being attributed to other artists. Carter v. Heilsmy-Spear, Inc., 71 F.3d 77, 81 (2d Cir.1995) (citing RALPH E. LERNER & JUDITH BRESLER, ART LAW 419-20 (1989)). "Rights of integrity" include the artist's right to prevent the modification, mutilation, or distortion of his work, and in some cases (if the work is of recognized stature), to prevent its destruction. Id. at 81-82 (citing ART LAW at 420-21).

Originating in nineteenth-century France, moral rights — le droit moral — are understood as rights inhering in the artist's personality, transcending property and contract rights and existing independently of the artist's economic interest in his work. See 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 8D.01[A] (2010); 5 WILLIAM F. PATRY, PATRY ON COPYRIGHT §§ 16:1, 16:3 (2010); John Henry Merryman, The Refrigerator of Bernard Buffet, 27 HASTINGS L.J. 1023, 1023-28 (1976). American copyright law, on the other hand, protects the economic interests of artists; Article I of the Constitution authorizes Congress "To Promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries." U.S. CONST. art. 1, § 8, cl. 8. Unlike other intellectual-property rights, moral rights are unrelated to the artist's pecuniary interests and are grounded in philosophical ideas about the intrinsic nature and cultural value of art rather than natural-property or utility justifications. See Carter, 71 F.3d at 81 (describing moral rights as "rights of a spiritual, non-economic and personal nature [that] ... spring from a belief that an artist in the process of creation injects his spirit into the work and that the artist's personality, as well as the integrity of the work, should therefore be protected and preserved"). VARA introduced a limited version of this European doctrine into American law, but it is not an easy fit.

VARA was enacted as a consequence of the United States' accession to the Berne Convention for the Protection of Literary and Artistic Works. After many years of resistance, the Senate ratified the treaty in 1988, bringing the United States into the Berne Union effective the following year. See 4 NIMMER § 17.01[C][2] (2010); 5 PATRY §§ 16:1, 16:3. The Berne Convention dates to 1886, when seven European nations (plus Haiti and Tunisia) joined together to extend copyright protection across their borders. See 4 NIMMER § 17.01[B][1] nn. 10 & 17 (2002). During the course of the next century, many other nations joined, and the treaty underwent periodic revisions, most notably for our purposes in 1928 when Article 6bis was added, incorporating the concept of moral rights. See 3 id. § 8D.01[B] (2004); 5 PATRY §§ 16:1, 16:3. Article 6bis provides:

(1) Independently of the author's economic rights, and even after the transfer of the said rights, the author shall have the right to claim authorship of the work and to object to any distortion, mutilation or other modification of, or other derogatory action in relation to, the said work, which would be prejudicial to his honor or reputation.

(3) The means of redress for safeguarding the rights granted by this Article shall be governed by the legislation of the country where protection is claimed.

When the United States joined the Berne Union in 1989, the concept of moral rights was largely unknown in American law. See Lee v. A.R.T. Co., 125 F.3d 580, 582 (7th Cir.1997) ("[I]t was accepted wisdom [before VARA] that the United States did not enforce any claim of moral rights."); see also Weinstein v. Univ. of Ill., 811 F.2d 1091, 1095 n. 3 (7th Cir.1987) (The Continental principle of le droit moral is a doctrine that "no American jurisdiction follows as a general matter."); Merryman, The Refrigerator of Bernard Buffet, 27 HASTINGS L.J. at 1035-36 ("The moral right of the artist, and in particular that component called the right of integrity of the work of art, simply does not exist in our law."). Article 6bis was a major obstacle to Berne ratification. See Martin v. City of Indianapolis, 192 F.3d 608, 611 (7th Cir.1999) (The treaty's moral-rights concept "was controversial in this country" and was embraced post-Berne only "in a very limited way."); Carter, 71 F.3d at 82-83 ("The issue of federal protection of moral rights was a prominent hurdle in the debate over whether the United States should join the Berne Convention").
American unease with European moral-rights doctrine — more particularly, the obligations imposed by Article 6bis — persisted beyond Berne ratification. Indeed, Congress initially took the position that domestic law already captured the concept in existing copyright and common-law doctrines and in the statutory law of some states. See Berne Convention Implementation Act of 1988, Pub.L. No. 100-568, §§ 2(2), (3), 102 Stat. 2853; 3 NIMMER § 8D.02[D][1] (2009); 5 PATRY § 16:3. This was seen as an implausible claim. See 3 NIMMER § 8D.02[D][1] ("The Congressional finding flies in the face of numerous judicial and scholarly pronouncements."); 5 PATRY § 16:3 (The American position that existing federal and state laws satisfied minimum Berne obligations created "a web of fictional compliance."). "[A] question of international credibility existed," and "some Berne co-Unionists ... expressed doubts regarding the accuracy or sincerity of the U.S. declaration that its law already afforded a degree of moral rights protection equivalent to Berne standards." Jane C. Ginsburg, Copyright in the 101st Congress: Commentary on the Visual Artists Rights Act and the Architectural Works Copyright Protection Act of 1990, 14 COLUM.-VLA J.L. & ARTS 477, 478-79 (1990). VARA was enacted to fill this perceived gap, but its moral-rights protection is quite a bit narrower than its European counterpart.

2. VARA’s scope

VARA amended the Copyright Act and provides a measure of protection for a limited set of moral rights falling under the rubric of "rights of attribution" and "rights of integrity" — but only for artists who create specific types of visual art. 17 U.S.C. § 106A(a). The statutory coverage is limited to paintings, drawings, prints, sculptures, and photographs created for exhibition existing in a single copy or a limited edition of 200 or less. See id. § 101 (defining "work of visual art"). The rights conferred by the statute exist independently of property rights; the artist retains them even after he no longer holds title to his work. Id. § 106A(a).

More specifically, VARA’s attribution and integrity rights are as follows:

(a) Rights of attribution and integrity. Subject to section 107 and independent of the exclusive rights provided in section 106, the author of a work of visual art —

(1) shall have the right —

(A) to claim authorship of that work, and

(B) to prevent the use of his or her name as the author of any work of visual art which he or she did not create;

(2) shall have the right to prevent the use of his or her name as the author of the work of visual art in the event of distortion, mutilation, or other modification of the work which would be prejudicial to his or her honor or reputation; and

(3) subject to the limitations set forth in section 113(d), shall have the right —

(A) to prevent any intentional distortion, mutilation, or other modification of that work which would be prejudicial to his or her honor or reputation, and any intentional distortion, mutilation, or modification of that work is a violation of that right, and

(B) to prevent any destruction of a work of recognized stature, and any intentional or grossly negligent destruction of that work is a violation of that right.

17 U.S.C. § 106A(a) (emphasis added). At issue here is the right of integrity conferred by subsection (a)(3)(A), which precludes any intentional modification or distortion of a work of visual art that "would be prejudicial to [the artist’s] honor or reputation."

A qualifying "work of visual art" is defined as:

(1) a painting, drawing, print, or sculpture, existing in a single copy, in a limited edition of 200 or fewer that are signed and consecutively numbered by the author, or, in the case of a sculpture, in multiple cast, carved, or fabricated sculptures of 200 or fewer that are consecutively numbered by the author and bear the signature or other identifying mark of the author; or

(2) a still photographic image produced for exhibition purposes only, existing in a single copy that is signed by the author, or in a limited edition of 200 copies or fewer that are signed and consecutively number by the author.
This definition also contains a number of specific exclusions: e.g., posters, maps, and globes; books, newspapers, magazines, and other periodicals; "motion picture[s] or other audiovisual work[s]"; merchandising and promotional materials; "any work made for hire"; and "any work not subject to copyright protection under this title." Id.

This last exclusion simply reinforces the point that VARA supplements general copyright protection: to qualify for moral rights under VARA, a work must first satisfy basic copyright standards. Under the Copyright Act of 1976, copyright subsists in "original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated." Id. § 102(a). "Works of authorship" include "pictorial, graphic, and sculptural works." Id. § 102(a)(5). VARA's definition of "work of visual art" is limited to a narrow subset of this broader universe of "pictorial, graphic, and sculptural works" that are otherwise eligible for copyright; only a select few categories of art get the extra protection provided by the moral-rights concept. 5 PATRY § 16:7 (2010) ("Protected `works of visual art' is a narrower subcategory of `pictorial, graphic, and sculptural works,' protected in section 102(a)(5).").

Several exceptions limit the scope of the rights granted under the statute:

(c) Exceptions. (1) The modification of a work of visual art which is a result of the passage of time or the inherent nature of the materials is not a distortion, mutilation, or other modification described in subsection (a)(3)(A).

(2) The modification of a work of visual art which is the result of conservation, or of the public presentation, including lighting and placement, of the work is not a destruction, distortion, mutilation, or other modification described in subsection (a)(3) unless the modification is caused by gross negligence.

17 U.S.C. § 106A(c) (emphasis added). The second of these — the "public presentation" exception — is at issue here. Another exception invoked by the Park District is found in a different section of the Copyright Act that defines the scope of a copyright owner's rights:

(d)(1) In a case in which —

(A) a work of visual art has been incorporated in or made part of a building in such a way that removing the work from the building will cause the destruction, distortion, mutilation, or other modification of the work as described in section 106A(a)(3), and

(B) the author consented to the installation of the work in the building either before the effective date set forth in section 610(a) of the Visual Artists Rights Act of 1990, or in a written instrument executed on or after such effective date that is signed by the owner of the building and the author and that specifies that installation of the work may subject the work to destruction, distortion, mutilation, or other modification, by reason of its removal,

then the rights conferred by paragraphs (2) and (3) of section 106A(a) shall not apply.

VARA rights cannot be transferred or assigned, but they can be waived in a writing signed by the artist and "specifically identify[ing] the work, and uses of that work, to which the waiver applies." Id. § 106A(e)(1). Absent a written waiver, the artist retains VARA rights during his lifetime even if he transfers ownership of the work or assigns his copyright.[5] Id. § 106A(d)(1), (e)(2).

3. Is Wildflower Works a painting or sculpture?

The district court held that Wildflower Works was both a painting and a sculpture but was insufficiently original to qualify for copyright. Alternatively, the court concluded that it was site-specific art and held that all site-specific art is implicitly excluded from VARA. Other arguments — in particular, whether Wildflower Works satisfies additional threshold requirements for copyright and whether VARA's public-presentation or building exceptions applied — were not reached.

On appeal Kelley contests the district court's conclusions regarding originality and site-specific art. The Park District defends these holdings and also reiterates the other arguments it made in the district court, except one: The Park District has not challenged the district court's conclusion that Wildflower Works is a painting and a sculpture.

This is an astonishing omission. VARA's definition of "work of visual art" operates to narrow and focus the statute's coverage; only a "painting, drawing, print, or sculpture," or an exhibition photograph will qualify. These terms are not further defined, but the overall
structure of the statutory scheme clearly illuminates the limiting effect of this definition. Copyright's broad general coverage extends to "original works of authorship," and this includes "pictorial, graphic, and sculptural works." 17 U.S.C. § 102(a)(5). The use of the adjectives "pictorial" and "sculptural" suggests flexibility and breadth in application. In contrast VARA uses the specific nouns "painting" and "sculpture." To qualify for moral-rights protection under VARA, Wildflower Works cannot just be "pictorial" or "sculptural" in some aspect or effect, it must actually be a "painting" or a "sculpture." Not metaphorically or by analogy, but really.

That Kelley considered the garden to be both a painting and a sculpture — only rendered in living material — is not dispositive. He also characterized it as an experiment in environmental theory, telling a reporter he was trying to "figure out the economic and ecological impact of introducing wildflowers into cities." In promoting Wildflower Works, Kelley variously described the project as a "living wildflower painting," a "study on wildflower landscape and management," and "a new vegetative management system that beautifies [the] landscape economically with low-maintenance wildflowers."

Kelley's expert, a professor of art history, reinforced his view that Wildflower Works was both a painting and a sculpture, but the district court largely disregarded her testimony as unhelpful. Kelley, "301 2008 WL 4449886, at *5. For its part the Park District initially marketed Wildflower Works as "living art," but this adds little to the analysis. VARA plainly uses the terms "painting" and "sculpture" as words of limitation. Even assuming a generous stance on what qualifies, see § 16:7 (suggesting a "liberal attitude toward what may be considered a painting, drawing, print, or sculpture"), the terms cannot be read coextensively with the broader categories of "pictorial" and "sculptural" works that are generally eligible for copyright under § 102(a)(5). If a living garden like Wildflower Works really counts as both a painting and a sculpture, then these terms do no limiting work at all.

The district judge worried about taking "too literalist an approach to determining whether a given object qualifies as a sculpture or painting." Kelley, 2008 WL 4449886, at *4. His concern was the "tension between the law and the evolution of ideas in modern or avant garden art; the former requires legislatures to taxonomize artistic creations, whereas the latter is occupied with expanding the definition of what we accept to be art." Id. We agree with this important insight. But there's a big difference between avoiding a literalist approach and embracing one that is infinitely malleable. The judge appears to have come down too close to the latter extreme.

4. Is Wildflower Works copyrightable?

To merit copyright protection, Wildflower Works must be an "original work[] of authorship fixed in a[] tangible medium of expression ... from which [it] can be perceived, reproduced, or otherwise communicated." 17 U.S.C. § 102(a). The district court held that although Wildflower Works was both a painting and a sculpture, it was ineligible for copyright because it lacked originality. There is a contradiction here. As we have explained, VARA supplements general copyright protection and applies only to artists who create the specific subcategories of art enumerated in the statute. VARA-eligible paintings and sculptures comprise a discrete subset of otherwise copyrightable pictorial and sculptural works; the statute designates these works of fine art as worthy of special protection. If a work is so lacking in originality that it cannot satisfy the basic requirements for copyright, then it can hardly qualify as a painting or sculpture eligible for extra protection under VARA. See Cronin, Dead on the Vine, 12 VAND. J. ENT. & TECH. L. at 239 ("[I]f a work does not evince sufficient original expression to be copyrightable, the work should belong in a category other than `visual art' as this term is contemplated under VARA.").

That point aside, the district court's conclusion misunderstands the originality requirement. Originality is "the touchstone of copyright protection today," an implicit constitutional and explicit statutory requirement. Feist Pub'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 347, 346, 111 S.Ct. 1282, 113 L.Ed.2d 358 (1991) ("Originality is a constitutional requirement."); id. at 355 (The Copyright Act of 1976 made the originality requirement explicit.); see also Schrock, 586 F.3d at 518-19 ("As a constitutional and statutory matter, [the sine qua non of copyright is originality.") (quoting Feist, 499 U.S. at 345, 111 S.Ct. 1282)). Despite its centrality in our copyright regime, the threshold for originality is minimal. See Feist, 499 U.S. at 345, 111 S.Ct. 1282; Am. Dental Ass'n v. Delta Dental Plans Ass'n, 126 F.3d 977, 979 (7th Cir.1997) ("The necessary degree of `originality' is low..."). The standard requires "only that the work was independently created by the author (as opposed to copied from other works), and that it possesses at least some minimal degree of creativity." Feist, 499 U.S. at 345, 111 S.Ct. 1282 (citation omitted). The "requisite level of creativity is extremely low; even
a slight amount will suffice. The vast majority of works make the grade quite easily, as they possess some creative spark." *Id.* (citation omitted).

The district court took the position that *Wildflower* Works was not original because Kelley was not "the first person to ever conceive of and express an arrangement of growing wildflowers in ellipse-shaped enclosed area[s]." *Kelley*, 2008 WL 4449886, at *6. This mistakenly equates originality with novelty; the law is clear that a work can be original even if it is not novel. *Feist*, 499 U.S. at 345, 111 S.Ct. 1282 ("Originality does not signify "303 novelty; a work may be original even though it closely resembles other works so long as the similarity is fortuitous, not the result of copying."). No one argues that *Wildflower* Works was copied; it plainly possesses more than a little creative spark.

The judge was also at a loss to discover "what about the exhibit is original. Is it the elliptical design? The size? The use of native plants? The environmentally-sustainable gardening method to which ‘vegetative management system' apparently refers?" *Kelley*, 2008 WL 4449886, at *6. It is true that common geometric shapes cannot be copyrighted. See U.S. COPYRIGHT OFFICE, COMPENDIUM II: COPYRIGHT OFFICE PRACTICES § 503.02(a)-(b) (1984); 2 PATRY § 4:17 (2010). And "[i]n no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such a work." 17 U.S.C. § 102(b).

The Park District suggests that *Wildflower* Works is an uncopyrightable "method" or "system," and is also ineligible because its design uses simple elliptical shapes. The first of these arguments is not well-developed; the second is misplaced. Although *Wildflower* Works was designed to be largely self-sustaining (at least initially), it's not really a "method" or "system" at all. It's a garden. And Kelley is seeking statutory protection for the garden itself, not any supposed "system" of vegetative management encompassed within it. Regarding the use of elliptical shapes, an author's expressive combination or arrangement of otherwise noncopyrightable elements (like geometric shapes) may satisfy the originality requirement. *Roulo v. Russ Berrie & Co.*, 886 F.2d 931, 939 (7th Cir.1989); 2 PATRY § 4:17 (Geometric shapes or symbols cannot themselves be protected, but an original creative arrangement of them can be.).

The real impediment to copyright here is not that *Wildflower* Works fails the test for originality (understood as "not copied" and "possessing some creativity") but that a living garden lacks the kind of authorship and stable fixation normally required to support copyright. Unlike originality, authorship and fixation are explicit constitutional requirements; the Copyright Clause empowers Congress to secure for "authors" exclusive rights in their "writings." U.S. CONST. art 1, § 8, cl. 8; see also 2 PATRY § 3:20 (2010) ("[T]he Constitution uses the terms 'writings' and 'authors;' 'originality' is not used."); *id.* § 3:22 (2010); 1 NIMMER § 2.03[A]-[B] (2004). The originality requirement is implicit in these express limitations on the congressional copyright power. See *Feist*, 499 U.S. at 346, 111 S.Ct. 1282 (The constitutional reference to "authors" and "writings" "[presuppose[s] a degree of originality."). The Supreme Court has "repeatedly construed all three terms in relation to one another [or] perhaps has collapsed them into a single concept"; therefore, "[w]ritings are what authors create, but for one to be an author, the writing has to be original." 2 PATRY § 3:20.

"Without fixation," moreover, "there cannot be a 'writing.'" *Id.* § 3:22. The Nimmer treatise elaborates:

> Fixation in tangible form is not merely a statutory condition to copyright. It is also a constitutional necessity. That is, unless a work is reduced to tangible form it cannot be regarded as a "writing" within the meaning of the constitutional clause authorizing federal copyright legislation. Thus, certain works of conceptual art stand outside of copyright protection.

*304 1 NIMMER § 2.03[B]. A work is "fixed" in a tangible medium of expression "when its embodiment in a copy or phonorecord ... is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration." 17 U.S.C. § 101. As William Patry explains:

> Fixation serves two basic roles: (1) easing problems of proof of creation and infringement, and (2) providing the dividing line between state common law protection and protection under the federal Copyright Act, since works that are not fixed are ineligible for federal protection but may be protected under state law. The distinction between the intangible intellectual property (the work of authorship) and its fixation in a tangible medium of expression (the copy) is an old and fundamental and important one. The distinction may be understood by examples of multiple fixations of the same work: A musical composition may be embodied in sheet music, on an audio-tape, on a compact disc, on a computer hard drive or server, or as part of a motion picture soundtrack. In each of the fixations, the intangible property remains a musical composition.
Finally, "authorship is an entirely human endeavor." Id. § 3:19 (2010). Authors of copyrightable works must be human; works owing their form to the forces of nature cannot be copyrighted. Id. § 3:19 n. 1; see also U.S. COPYRIGHT OFFICE, COMPENDIUM II: COPYRIGHT OFFICE PRACTICES § 503.03(a) ("[A] work must be the product of human authorship* and not the forces of nature.) (1984); id. § 202.02(b).

Recognizing copyright in Wildflower Works presses too hard on these basic principles. We fully accept that the artistic community might classify Kelley's garden as a work of postmodern conceptual art. We acknowledge as well that copyright's prerequisites of authorship and fixation are broadly defined. But the law must have some limits; not all conceptual art may be copyrighted. In the ordinary copyright case, authorship and fixation are not contested; most works presented for copyright are unambiguously authored and unambiguously fixed. But this is not an ordinary case. A living garden like Wildflower Works is neither "authored" nor "fixed" in the senses required for copyright. See Toney v. L'Oreal USA, Inc., 406 F.3d 905, 910 (7th Cir.2005) ("A person's likeness — her persona — is not authored and it is not fixed."); see also Cronin, Dead on the Vine, 12 VAND. J. ENT. & TECH. L. at 227-39.

Simply put, gardens are planted and cultivated, not authored. A garden's constituent elements are alive and inherently changeable, not a fixed copy of the gardener's intellectual property. Although the planting material is tangible and can be perceived for more than a transitory duration, it is not stable or permanent enough to be called "fixed." Seeds and plants in a garden are naturally in a state of perpetual change; they germinate, grow, bloom, become dormant, and eventually die. This life cycle moves gradually, over days, weeks, and season to season, but the real barrier to copyright here is not temporal but essential. The essence of a garden is its vitality, not its fixedness. It may endure from season to season, but its nature is one of dynamic change.

We are not suggesting that copyright attaches only to works that are static or fully permanent (no medium of expression lasts forever), or that artists who incorporate natural or living elements in their work can never claim copyright. Kelley compares Wildflower Works to the Crown Fountain, a sculpture by Spanish artist Jaume Plensa that sits nearby in Chicago's Millennium Park. The surfaces of Plensa's fountain are embedded with LED screens that replay recorded video images of the faces of 1,000 Chicagoans. See http://www.explorechicago.org/city/en/ things see do attractions/dca_tourism/ Crown_Fountain.html (last visited Feb. 10, 2011). But the Copyright Act specifically contemplates works that incorporate or consist of sounds or images that are broadcast or transmitted electronically, such as telecasts of sporting events or other live performances, video games, and the like. See 17 U.S.C. § 101 (defining "fixed" as including a "work consisting of sounds, images, or both, that are being transmitted... if a fixation of the work is being made simultaneously with its transmission"); see also Balt. Orioles, Inc. v. Major League Baseball Players Ass'n, 805 F.2d 663, 675 (7th Cir.1986); Midway Mfg. Co. v. Artic Int'l, Inc., 704 F.2d 1009, 1013-14 (7th Cir.1983).

Wildflower Works does not fit in this category; the Crown Fountain is not analogous.

Though not addressing the requirement of fixation directly, the district court compared Wildflower Works to "[t]he mobiles of Alexander Calder" and "Jeff Koons' "Puppy," a 43-foot flowering topiary." Kelley, 2008 WL 4449886, at *4. These analogies are also inapt. Although the aesthetic effect of a Calder mobile is attributable in part to its subtle movement in response to air currents, see http://en.wikipedia.org/ wiki/Alexander_Calder (last visited Feb. 10, 2011), the mobile itself is obviously fixed and stable. In "Puppy"
the artist assembled a huge metal frame in the shape of a puppy and covered it with thousands of blooming flowers sustained by an irrigation system within the frame. See http://en.wikipedia.org/wiki/Jeff_Koons (last visited Feb. 10, 2011). This may be sufficient for copyright (we venture no opinion on the question), but Wildflower Works is quite different. It is quintessentially a garden; “Puppy” is not.

In short, Wildflower Works presents serious problems of authorship and fixation that these and other examples of conceptual or kinetic art do not. Because Kelley’s garden is neither “authored” nor “fixed” in the senses required for basic copyright, it cannot qualify for moral rights protection under VARA.

5. Site-specific art, and the public-presentation and building exceptions

This case also raises some important questions about the application of VARA to site-specific art, as well as the statute’s public-presentation and building exceptions. Though we need not decide these questions, we do have a few words of caution about the district court’s treatment of the issue of VARA and site-specific art. The court classified Wildflower Works as a form of site-specific art; we see no reason to upset this factual finding. The court then adopted the First Circuit’s holding in Phillips that site-specific art is categorically excluded from VARA. This legal conclusion is open to question.

Phillips involved a VARA claim brought by artist David Phillips in a dispute over a display of 27 of his sculptures in Boston’s Eastport Park across from Boston Harbor. Phillips v. Pembroke Real Estate, Inc., 459 F.3d 128, 130 (1st Cir. 2006). A planned redesign of the park called for the removal and relocation of Phillips’s sculptures; he sought an injunction under VARA, claiming the removal of his sculptures would violate his right of integrity. Id. at 131. The district court held that although the sculptures qualified as a single integrated work of visual art, park administrators were entitled to remove them under VARA’s public-presentation exception. Id. at 138-39. The First Circuit affirmed on alternative grounds, holding that VARA does not apply to any site-specific art.

The court based this holding on a perceived irreconcilable tension between the public-presentation exception and the purpose of site-specific art: “By definition, site-specific art integrates its location as one of its elements. Therefore, the removal of a site-specific work from its location necessarily destroys that work of art.” Id. at 140. Under the public-presentation exception, a modification of a work of visual art stemming from a change in its “public presentation, including lighting or placement,” is not actionable unless it is caused by gross negligence. If VARA applied to site-specific art, the First Circuit reasoned, then the statute would “purport[] to protect site-specific art” but also “permit its destruction by the application” of the public-presentation exception. Id. The court held that “VARA does not protect site-specific art and then permit its destruction by removal from its site pursuant to the statute’s public presentation exception. VARA does not apply to site-specific art at all.” Id. at 143.

There are a couple of reasons to question this interpretation of VARA. First, the term "site-specific art" appears nowhere in the statute. Nothing in the definition of a "work of visual art" either explicitly or by implication excludes this form of art from moral-rights protection. Nor does application of the public-presentation exception operate to eliminate every type of protection VARA grants to creators of site-specific art; the exception simply narrows the scope of the statute's protection for all qualifying works of visual art. The exception basically provides a safe harbor for ordinary changes in the public presentation of VARA-qualifying artworks; the artist has no cause of action unless through gross negligence the work is modified, distorted, or destroyed in the process of changing its public presentation.

Second, Phillips's all-or-nothing approach to site-specific art may be unwarranted. Site-specific art is not necessarily destroyed if moved; modified, yes, but not always utterly destroyed. Moreover, some of VARA’s protections are unaffected by the public-presentation exception. An artist's right of integrity can be violated in ways that do not implicate the work's location or manner of public presentation; site-specific art — like any other type of art — can be defaced and damaged in ways that do not relate to its public display. And the public-presentation exception does nothing to limit the right of attribution, which prevents an artist's name from being misappropriated.

Then there is the matter of the building exception, which applies to works "incorporated in or made part of a building in such a way that removing the work from the building will cause the destruction, distortion, mutilation, or other modification of the work." 17 U.S.C. § 113(d)(1)(A). These works do not get moral-rights protection if the artist: (1) consented to the installation of his work in the building (if pre-VARA); or (2) executed a written acknowledgment that removal of the work may subject it to destruction, distortion, mutilation, or modification (if post-VARA). Id. § 113(d)(1)(B). On its face this exception covers a particular kind of site-specific art. Its presence in the statute suggests that site-specific art is not categorically excluded from VARA. [81]
These observations are of course general and not dispositive. Because we are resolving the VARA claim on other grounds, we need not decide whether VARA is inapplicable to site-specific art.

B. The Park District's Cross-Appeal on the Contract Claim

The Park District challenges the judgment against it for breach of contract even though damages were assessed at a nominal $1. The district court held that Commissioner Burroughs's casual remark — "You're still there, aren't you? That's all you need to do." — created an implied-in-fact contract requiring the Park District to give Kelley reasonable notice before reconfiguring Wildflower Works. Although factual findings about the existence of a contract are reviewed for clear error, ReMapp Int'l Corp. v. Comfort Keyboard Co., 560 F.3d 628, 633 (7th Cir. 2009), there is a threshold legal question here about the commissioner's unilateral authority to bind the Park District to a contract. Our review is de novo. See Manning v. United States, 546 F.3d 430, 432 (7th Cir. 2008).

Two statutes guide our analysis. The first is the Chicago Park District Act, which provides in relevant part that "[t]he commissioners of [the Park District] constitute the corporate authorities thereof, and have full power to manage and control all the officers and property of the district, and all parks, driveways, boulevards and parkways maintained by such district or committed to its care and custody." 70 ILL. COMP. STAT. 1505/7.01. The district court noted the statute's use of the plural "commissioners" and "authorities" and concluded from this that each individual commissioner was a separate corporate "authority" with the power to unilaterally bind the Park District.

This conclusion strains the statutory language and ignores how public bodies customarily operate. It also contradicts another provision in the Illinois Park District Code, which applies to all Illinois park districts and must be read in conjunction with the Chicago Park District Act. The Illinois Park District Code states:

No member of the board of any park district ... shall have power to create any debt, obligation, claim or liability, for or on account of said park district... except with the express authority of said board conferred at a meeting thereof and duly recorded in a record of its proceedings.

70 ILL. COMP. STAT. 1205/4-6 (emphasis added). When read together, these statutes confirm that there is only one corporate authority of the Chicago Park District — its Board of Commissioners — and that individual commissioners cannot unilaterally bind the Park District's Board to a contract without express Board approval.

There is no evidence that the Park District's Board of Commissioners authorized Commissioner Burroughs to enter into a contract with Kelley. Moreover, Illinois law provides that ultra vires contracts entered into by municipal corporations are invalid, see, e.g., McMahon v. City of Chicago, 339 Ill. App. 3d 41, 273 Ill. Dec. 447, 789 N.E.2d 347, 350 (2003), so Commissioner Burroughs's offhand remark cannot have created a valid implied-in-fact contract. The judgment for Kelley on the contract claim was premised on legal error; the Park District was entitled to judgment on this claim.

For the foregoing reasons, we AFFIRM the judgment in favor of the Park District on the VARA claim; we REVERSE the judgment in favor of Kelley on the contract claim and REMAND with instructions to enter judgment for the Park District.

[1] The complaint also alleged that the Park District's actions constituted an unlawful taking, but the district court dismissed this count prior to trial. The takings claim is not at issue on appeal.


[5] VARA applies to works created after its effective date (June 1, 1991, six months after its December 1, 1990 date of enactment) and works created before its effective date "but title to which has not, as of such effective date, been transferred from the author." Visual Artists Rights Act of
Wildflower Works was created before VARA's effective date, but the parties stipulated that Kelley owns the planting material. Kelley has not executed a written waiver of VARA rights.

Among other things, the expert testified that Wildflower Works was both a painting and a sculpture because "three dimensional objects become two dimensional paintings when viewed from airplanes," an assertion the district court characterized as "strange." Kelley v. Chi. Park Dist., No. 04 C 07715, 2008 WL 4449886, at *5 (N.D.Ill. Sept. 29, 2008).

The district court basically concluded that the term "sculpture" included any three-dimensional art form — that is, any "non-two dimensional" work that can be called "art." Kelley, 2008 WL 4449886, at *5. As we have noted, this expansive approach fails to distinguish between "sculptural works," included in the broad subject matter of copyright, and VARA's use of the more limited term "sculpture." As for "painting," the judge consulted this verb definition for "paint": 

- "[1] to apply color, pigment, or paint to ... [2] to produce in lines and colors on a surface by applying pigments, [3] to depict by such lines and colors, [4] to decorate, adorn, or variegate by applying lines and colors." Id. (quoting Merriam-Webster's Online Dictionary, http://www.m-w.com/dictionary/paint[1] (last visited September 25, 2008)). The judge then characterized Wildflower Works as "[a]n exhibit that corrals the variegation of wildflowers into pleasing oval swatches" and concluded from this that the garden "could certainly fit within some of the[se] ... definitions of a painting." Id.

As we have explained, however, VARA's definition of a "work of visual art" uses nouns, not verbs. The noun "painting" is more precise than the verb "paint." A "painting" is:

1.a. Painted matter; that which is painted; ... a representation on a surface executed in paint or colours; a painted picture or likeness. b. The representing of a subject on a surface by the application of paint or colours; the art of making such representations; ... the practice of applying paint to a canvas, etc., for any artistic purpose.


1.a.... the process or art of carving or engraving a hard material so as to produce designs or figures in relief, in intaglio, or in the round. In modern use, that branch of fine art which is concerned with the production of figures in the round or in relief, either by carving, by fashioning some plastic substance, or by making a mould for casting in metal; the practice of this art.... 2. concr. a. The product of the sculptor's art; that which is sculptured (or engraved); sculptured figures in general. b. In particularized sense: A work of sculpture; a sculptured (or engraved) figure or design.

Sculpture Definition, id., http://www.oed.com/viewdictionaryentry/Entry/173877 (last visited Feb. 10, 2011). A living garden might be said to have "painterly" or "sculptural" attributes, but it's hard to classify a garden as a "painting" or "sculpture" as these terms are commonly understood.

The Park District argued that the building exception applied to Wildflower Works because the garden is located on top of the Monroe Street parking garage and accommodates the air vents that provide ventilation to the garage below. This strikes us as something of a reach. Wildflower Works is not "incorporated into" or "made part of" the parking garage; it is situated on top of it.
Virtual Reality And The Law: Part 1

By David Fink and Jamie Zagoria, Kelley Drye & Warren LLP

Law360, New York (January 11, 2017, 1:39 PM EST) -- In case you have been living under a rock, virtual reality (VR) and its first cousin, augmented reality (AR), have arrived.

The highly publicized and long-awaited head-mounted displays (HMDs), the headsets through which the world of virtual reality can be accessed, have been or will be very soon be made available for sale to the public, such as Facebook-owned Oculus VR's Oculus Rift, Samsung's Gear VR, Sony's PlayStation VR and HTC's Vive.

In other words, VR/AR is going mainstream. Nearly all of the top 10 tech companies, including Apple, Google, Samsung and Microsoft, have jumped on the VR bandwagon, investing significantly in the space. Countless players across many different industries, including Marriott, Netflix, Hulu, Birchbox and Ford, have developed VR “experiences,” seeking to capitalize on the hype.

Indeed, 75 percent of the 100 companies on Forbes’ World’s Most Valuable Brands list have either developed VR or AR experiences for their customers or employees, or have invested in developing the technology.[1] Television networks have broadcast sporting events such as the Kentucky Derby, NASCAR and the NBA live in VR. The 2016 Sundance and Cannes Film Festivals featured VR short films.

The Coachella music festival provided each 2016 attendee with a custom cardboard VR headset, allowing them to explore the festival grounds and preview performances through the Coachella VR app. Six Flags debuted the New Revolution, a roller coaster experience during which riders wear a VR headset while riding a roller coaster. As the foregoing examples demonstrate, VR is the new “it” technology, and “it” is everywhere.

Even in its nascent state, VR is proving to have a multitude of beneficial uses stemming far beyond the gaming industry with which it is most readily associated. The healthcare industry is using VR to treat human cognitive and behavioral conditions and provide training to medical students. The real estate and automotive industries are using VR to show properties and cars to potential buyers.

The sports industry uses VR to provide zero-impact training to athletes. Educators are incorporating the technology into learning tools designed to engage children. VR is also being utilized for advertising, space exploration, tourism, military and law enforcement purposes and, naturally, entertainment.

In contrast to the virtual world they exploit, however, the new HMDs, as well as VR/AR in general, raise very real legal issues, especially in the areas of consumer safety, privacy, intellectual property and First Amendment law.

Most recently, Pokémon Go, which was released to the public on July 6, 2016, has captured so much attention that it borders on mania.[2] For the uninformed, Pokémon Go is a game that uses the player’s smartphone camera and augmented reality to insert virtual Pokémon (fictitious creatures) into the user’s real world.
The game designates real-world locations, such as buildings and landmarks, as in-game destinations; players are encouraged to walk around their community in order to locate and capture these Pokémon. Pokémon Go has produced some beneficial effects, such as promoting physical exercise, generating revenue for businesses and assisting law enforcement in apprehending suspects.

It has also foreshadowed the problems that future VR/AR games and devices may create. For example, cell-phone-fixated players have walked into streets without looking. Some are driving while playing the game — indeed, one player crashed into a tree due to playing Pokémon Go while driving. [3] Players have also attempted to capture Pokémon located in inappropriate places such as the Holocaust Museum and the 9/11 Memorial.

At least one man’s private residence has been marked by the app as an in-game destination, causing players to congregate outside of his home at all times of the day.[4] Armed robbers have used the game to bait unsuspecting players into unpopulated areas. A teenage girl in Wyoming even discovered a dead body while trying to catch a water Pokémon.[5]

For at least a few days, the app contained a coding "error" that gave the game’s developer “full access” to users’ Google accounts, including Gmail.[6] Remarkably, all of the foregoing events happened over the course of the first week Pokémon Go was available to the public. The fact that Pokémon Go became ubiquitous in such a short period of time is a testament to public appetite for VR/AR.

Below, we highlight some prospective issues raised by VR/AR, while recognizing that this discussion is pure conjecture at this point. The world of VR is still in its infancy, and, as such, these legal issues have not yet been fully explored in connection with VR.

While we can (and do below) compare VR to other forms of media and technology preceding it, VR is unlike anything before it in terms of the immersive and interactive experience it provides. As such, it is difficult to predict all of the legal implications of this new technology.

As HMDs and other VR devices become ubiquitous, these and other issues will come to the forefront and legislation and case law will likely provide answers to many outstanding questions. Only time will tell us which issues are non-issues and which issues require further regulation, innovation and attention.

**Consumer Safety**

While the fully immersive experience of VR is what makes it unique and appealing, it has also spawned perhaps the top (and most obvious) concern regarding VR — the physical risks involved. It is not difficult to imagine the kind of harm that can ensue when an HMD user proceeds to move around a room filled with furniture, pets, cords, walls and other objects while her view of the real world is obstructed.

Injury to both the user and others in the vicinity is foreseeable. The internet is filled with reports and videos of HMD users running into walls, furniture, the ceiling and other people. The risk of harm is especially high when the user is engaged in a VR experience that encourages moving around (e.g., when the goal is above the user).

It is not only real-world objects that can cause the VR user harm, but objects within the virtual space, as well; forgetting that these objects are not real, VR users have attempted to sit or lean on nonexistent furniture and are quickly jolted back to reality when they fall onto the very real floor.

If these physical risks actualize and HMDs begin causing serious consumer injuries, a slew of product liability lawsuits will likely emerge claiming that these products suffer from a design defect and/or fail to sufficiently warn of their risks. It is foreseeable that future plaintiffs will claim that HMDs are defective in design under both strict liability and negligence theories.

But a product does not suffer from a design defect solely because it is dangerous (e.g., a knife). Like a knife, while the HMD’s design, essentially a high-tech blindfold, certainly presents a risk of danger, it also serves VR’s primary purpose — to fully immerse the user in a virtual experience.
On the other hand, some HMD creators have shown that these products can be made safer with minimal interruption to the immersive VR experience. Indeed, Valve created a safety mechanism for its HTC Vive called the Chaperone System, which utilizes the Vive’s front-facing camera to detect physical objects in the user’s path.[7] It also enables users to define the area of the room that they will use and notifies them when they get close to the boundary.[8]

Unlike the Vive, the first consumer version of the Oculus Rift does not come with a Chaperone type system or a front-facing camera. The Rift, therefore, cannot detect or prevent a user from colliding with physical objects in their path, such as walls, tables, and chairs.[9]

This raises the question: is an HMD’s lack of a front-facing camera or chaperone system a design defect? In other words, could Oculus be held liable if a Rift user suffers a physical injury that could have been prevented by the inclusion of a front-facing camera and/or a Chaperone system?

When asked if the Rift can set boundaries to ensure that users do not walk into walls, Oculus’ founder indicated that he believed that to be a software issue rather than a hardware issue.[10] Interestingly, however, at least one earlier model of the Rift had a front-facing camera.[11] Further, user reports and videos clearly indicate that Rift users are getting up and walking around, and several users are claiming that the Rift is dangerous and needs a Chaperone system like the Vive.

Oculus could take the position that the doctrine of assumption of risk bars liability for any injury that results from consumers walking around while wearing the Rift. Oculus could argue that not only is the risk of injury foreseeable, but it specifically warns users of such risks in its health and safety warnings.

Thus, so the argument would go, the consumer assumed the risk of injury because they were aware of it and still used the HMD. The success of this argument would likely depend on several factors, including the adequacy of Oculus’ health and safety warnings and whether the inclusion of a front-facing camera is economical.

Manufacturers of HMDs may be able to avoid liability for injuries and side effects resulting from HMD usage by providing specific and thorough health and safety warnings. The health and safety warnings that accompany HMDs already on the market, such as the Rift and Vive, alert consumers to the immersive nature of VR and the risk of serious injury if the product is used in an unsafe area (or if one relies upon imaginary furniture to bear their weight).

These warnings also notify consumers that VR interaction may produce a multitude of negative side effects, ranging from nausea and headaches to seizures and post-traumatic stress disorder. These types of consumer safety warnings insulated Nintendo from liability in connection with its Wii remotes, and it stands to reason that they will similarly prevent the imposition of liability in connection with VR HMDs.[12] Future claims will either confirm the adequacy of such warnings or will test their limits.

Furthermore, since VR only recently made its public introduction, it may involve risks that are not yet known, including the long-term effects of VR usage. While more research is needed, many believe that long-term VR engagement may have an impact on eyesight, cognition and behavioral function, especially in children.

There are also concerns that the wholly-immersive nature of VR will cause users to develop serious addictions that could lead to death from exhaustion, dehydration or starvation.[13] The threat of addiction to VR does not seem so far-fetched when one considers the severe addictions that users have developed to the significantly less immersive massively multiplayer online games (MMOGs).[14]

Oculus warns users to “take at least a 10 to 15 minute break every 30 minutes, even if you don’t think you need it,” but does not specifically mention anything about the threat of addiction.[15] Warnings may be modified or enhanced to address these and other concerns as they arise, or may betested in future litigation.

As with all new technology, refinements in both the technology and the business and legal practices surrounding it will continue for as long as the technology is interesting to developers and consumers.
In the second part of this article, we will consider the legal implications of VR and AR with respect to privacy, intellectual property and First Amendment issues.

David E. Fink is managing partner of Kelley Drye & Warren LLP’s Los Angeles office and former chair of the firm’s media and entertainment practice group. His practice includes business, employment and entertainment matters, with an emphasis on First Amendment, entertainment and intellectual property litigation.

Jamie N. Zagoria is an associate in the firm’s Los Angeles office. Her practice focuses on entertainment, intellectual property and complex business litigation.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

Virtual Reality And The Law: Part 2

By David Fink and Jamie Zagoria, Kelley Drye & Warren LLP

Law360, New York (January 12, 2017, 11:03 AM EST) -- In case you have been living under a rock, virtual reality (VR) and its first cousin, augmented reality (AR), have arrived. Nearly all of the top 10 tech companies, including Apple, Google, Samsung and Microsoft, have jumped on the VR bandwagon, investing significantly in the space.

In the first part of this article, we examined possible consumer protection issues raised by VR and AR technologies. In this installment, we will consider the legal implications of VR and AR with respect to privacy, intellectual property and First Amendment issues.

Privacy

Like many mainstream products on the market today, HMDs such as Oculus’ Rift can — and do — collect data about their users. Unlike other forms of technology, however, the new VR HMDs have an unprecedented ability to collect unique personal information that consumers are not accustomed to providing, namely, physical movement.

Oculus’ privacy policy reveals that the company not only collects information provided by its users, but also automatically collects certain information when a consumer uses Oculus’ services, including “information about your physical movements and dimensions when you use a virtual reality headset.”[1]

In addition to user location, Oculus tracks users’ head, hand and eye movements, and can determine if a user is sitting or standing. Moreover, the software required to run the Rift includes an internet-connected process that is continuously running and routinely sending information to Facebook’s servers, even when the user is not using the device.[2]

In other words, Facebook, through Oculus, knows what content users are viewing on Rift, where they are viewing it, and the positional tracking of the HMD.[3] Concerns over user privacy and security have already been articulated.

Growing concerns over Oculus’ privacy policy caused Senator Al Franken to ask Oculus’ CEO, Brendan Iribe, some hard questions regarding “the company’s collection, storage, and sharing of users’ personal data” to enable consumers to “make informed decisions about whether and with whom they share such sensitive information.”[4]

Oculus responded that it “collects information about physical dimensions to help improve its services” and admitted that it shares such information with its developers, including Facebook, “as necessary to provide our services and enhance the ability of relevant VR products for people.”[5] Notably, however, Oculus did not address whether it sells such information to third parties, despite being specifically questioned on the subject.

The unique (and arguably sensitive) information collected through VR products will likely be coveted by advertisers, hackers and potentially government agencies.
VR companies that collect this data must be careful not to mislead consumers by failing to implement or maintain “reasonable” and “appropriate” controls to secure such information, or by making materially misleading statements or deceptive omissions of material facts to consumers concerning the use, disclosure or safeguarding of such information (e.g., in a privacy policy or other public-facing materials). Otherwise, they could be subject to enforcement actions by the Federal Trade Commission, as well as litigation brought by consumers for invasion of privacy.

Those selling VR products and experiences will be well served by providing clear policies and choices with respect to the information collected. Responsible safeguarding of private information collected from users will also protect consumers and insulate developers from liability. No matter what policies and practices are adopted, the trove of information collected from the marketplace of VR users will make a tempting target for hackers and thieves.

In this respect, the emerging VR community will not be breaking new ground; it will merely be joining the ranks of countless other interactive businesses who are entrusted with protecting customer information. A wide range of businesses, from banking and credit card companies to entertainment and dating services, already struggle to balance the quality of the services and products they provide against the need to protect user privacy.

**Intellectual Property**

VR may also implicate intellectual property issues where the virtual environment contains real world corporate logos, copyrighted works or a person’s name or likeness. As with video games, the laws of copyright, trademark and right of publicity govern the use of such content in VR.

A copyright owner has the exclusive right to reproduce, distribute, perform or display the copyrighted work, or to prepare derivative works based on that work.[6] Thus, VR content creators must secure a license from the applicable rights owner before displaying or performing material subject to copyright protection within a VR experience.[7]

Likewise, software developers must be cautious when it comes to enabling VR users to generate content (such as avatars). If users are provided with the means to incorporate protected material into the content they create, software developers may be held secondarily liable for the user’s infringing conduct.

With respect to the use of another’s trademark in VR, solely including another’s mark in VR is not per se trademark infringement. Rather, the mark’s owner would have to establish the mark was used “in commerce” in order to state a claim for trademark infringement. For instance, if a VR user sells virtual cars bearing the BMW logo to other VR users, the use of the mark may be found to meet the “in commerce” element of trademark infringement.

Similarly, invoking the name or likeness of a celebrity in VR could amount to an unauthorized use — forming the basis for a right of publicity action — if the use was commercial in nature. Because right of publicity laws vary from state to state, content providers must take additional care to ensure that use stays within the bounds of the law in every jurisdiction in which the products are distributed.

Addressing this inconsistency is a common issue in the creation of entertainment and other creative content already, and that problem will remain a concern with respect to VR products.

As far as intellectual property issues in the virtual space are concerned, it appears that existing law will apply to protect the intellectual property rights of owners in the virtual world. If VR content is deemed to be an expressive work, however, as with video games, the First Amendment may provide a defense to future intellectual property lawsuits arising out of the use of a trademark, a copyrighted work or a person’s name or likeness within VR.

**First Amendment Issues**

Like movies, television, books and other expressive works before it, VR communicates ideas. Given that the Supreme Court has held that even violent video games qualify for First Amendment protection,[8] it would seem that, by extension, most VR content should receive First Amendment protection as well.
The highly immersive and interactive nature of VR, however, is encouraging the creation of some content that is less clearly within the protection of the First Amendment.

For instance, the adult film industry is developing X-rated VR experiences that seek to turn pornography into an active experience. But the non-PG VR uses go far beyond ordinary pornography. VR users may be able to engage in behavior that is illegal and unacceptable in the real world, such as virtual prostitution, torture, murder and other illegal sexual activities.

This dark side of VR raises many moral and legal questions. It is foreseeable that legislators will be called upon to regulate VR to preclude user access to some types of experiences, which will surely garner the attention of First Amendment advocates.

VR is lauded by users for the realistic and completely immersive experiences it provides. For example, users participating in a horror-themed VR experience display palpable signs of fear, signifying that the experience is quite real.

By analogy, performing illegal acts in the virtual yet life-like world that one rarely, if ever, gets to perform in the real world would arguably feel even more real to the user and bring the action closer to a real-life crime.

It is unclear whether VR’s incomparable realness and interactivity, coupled with the obscene nature of certain VR content, would render such content outside of the First Amendment’s protective cloak.

**Conclusion**

Because VR and the new HMDs have only recently gone public, many interesting issues arise as new uses and experiences with VR are created and reported. The number of products, experiences, and services utilizing VR will certainly continue to explode in the near future as the technology evolves, and so will the legal issues surrounding it.

As with any new technology, some anticipated hurdles will turn out to be non-issues, while other issues may arise and surprise everyone. With all of the uncertainty surrounding VR, one thing that can be said with confidence is that we have only just begun — and a new world of technology and law lies ahead.

---

*David E. Fink is managing partner of Kelley Drye & Warren LLP's Los Angeles office and former chair of the firm's media and entertainment practice group. His practice includes business, employment and entertainment matters, with an emphasis on First Amendment, entertainment and intellectual property litigation.*

*Jamie N. Zagoria is an associate in the firm’s Los Angeles office. Her practice focuses on entertainment, intellectual property and complex business litigation.*

*The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.*


[7] Unless such use comes under the “fair use” doctrine of copyright law, which will require a fact-intensive analysis of the use.

Commentary: Pokemon Go hotspots: 'Virtual trespassing' in real-world lawsuit

Have Pokemon Go players trampled your yard or overrun your business looking for virtual characters? Do you consider it trespassing? Some homeowners do. As the Wall Street Journal reports, a federal judge will decide if a lawsuit can go forward that charges the game’s developers with violating trespass and negligence laws. The issue is software that sends users to specific locations. To learn more about the law, and the implications of the lawsuit, the Orlando Sentinel Editorial Board engaged Shawn Bayern, a law professor at Florida State University.

Q: You’ve described the law as very messy, and that each state handles it differently. What makes Florida’s law different?
A: It’s not that Florida’s is different in a systematic way. It’s just that the law concerning things like “trespass” and “nuisance” can be very messy, and states often differ in the details. If I had to make a broad statement, it’s often harder for plaintiffs to win tort lawsuits in Florida than in other states. Some other states have developed legal doctrines over the last 50 years that are more protective of plaintiffs.

Q: Can you describe the case brought by residents of the Villas of Positano in South Florida?

A: Essentially, their argument is that the Pokémon Go app led players to their property, causing damage and loss of “use and enjoyment” of the property. There are a variety of ways you can make this argument under law, but I personally think that “negligence law” is the most appealing.

If you generalize a bit, you can think of the argument like this: We all know that if you drive a truck negligently and cause property damage, the law will make you pay for it. What if you design an app carelessly and cause the same type of property damage? Should you be responsible for that?

One big difference with a careless app is that your harm is less “direct”; it involves other people whom you don’t control. But the law already recognizes many situations where you can be responsible for carelessly creating situations that make it more likely that third parties will hurt people. For example, an apartment building might be responsible for adopting negligent security practices, increasing the risk of crime to its residents. In one case in California, a radio station with a large young audience was held liable when it held a contest that encouraged highway drivers to be the first to find a roving, mobile radio transmitter, and some young drivers got into an accident as a result. I can easily imagine future app cases quite similar to that.

Q: Is it realistic to conclude that Niantic can control Pokémon Go player’s real-world movements?

A: The reason I think “negligence” law makes the most sense here is that it’s not necessarily about control. Obviously if the makers of an app intentionally induce other people to commit trespass, that’s wrong. But the makers of an app can still be careless in leading other people to act in harmful or dangerous ways, just by being thoughtless in how they create the app. To put it simply, you don’t have to be able to control anyone for a court to find that you acted unreasonably in creating a risk of damage or danger.

It’s worth adding that an app maker can still be careless even if it makes players sign a form that says they promise not to trespass or do anything illegal, as I believe the defendants did here. In general, negligence law looks at the defendant’s conduct overall. It might be a good idea to tell players to behave safely, but that shouldn’t be a magical formula to protect you from liability if you’ve otherwise been careless in setting up a game.

“An app maker can still be careless even if it makes players sign a form that says they promise not to...
Q: What are the broader implications for makers of games or other software that sends users to specific locations? What would be the practical effect on gaming technology and players from ruling against Niantic?

A: Of course, everyone likes legal rules that exempt them from any possible liability. That gives peace of mind and prevents them from having to pay to defend against meritless lawsuits. But all negligence law requires, in general, is that you behave reasonably. In other words, the problem isn’t publishing an app that tells people to go to a specific location; the problem is doing that in a way that unreasonably risks harm to people or property.

Q: Have laws — or court rulings — caught up with advances in technology and software? What advice would you have for Florida lawmakers to update trespass laws? Should they cover only physical intrusions or virtual ones?

A: One nice thing about the common law — the way judges respond to new cases and extend existing doctrines — is that it can be very flexible. Judges should always be open to applying existing doctrines in new ways to suit advances in technology. Here, negligence law is quite an adaptable tool. If our general rule is “if you act unreasonably and cause personal injury or property damages as a result, you have to pay for it,” that seems to extend pretty well into at least some new technologies.

I’d be more skeptical of the need, at the moment, of claims that are more like “virtual trespass.” If a game wants to let me wander around a map and pretend to be walking on other people’s property while I’m sitting at home, that shouldn’t be a problem. The concern is that an app can cause real-world damage, and that harm is no less real just because it’s caused by third-party players of a game.

Of course, there are many environments where virtual things are quite valuable on their own. For example, my understanding is that there are some games where “real estate” in the game — purely virtual property — sells for significant sums of real-world dollars. Protecting that sort of virtual property might become a significant issue for the law in the future.
Women use the Oculus Rift DK2 at the Westfield Shopping Centre in London / Tim P. Whitby/Getty Images for Westfield

The Facebook-owned company’s VR headset installs a piece of software that keeps watch of when people are using it — and can send that off to other firms

OCULUS RIFT TERMS AND CONDITIONS ALLOW FACEBOOK TO MONITOR USERS’ MOVEMENTS AND USE IT FOR ADVERTISING

The Facebook-owned company’s VR headset installs a piece of software that keeps watch of when people are using it — and can send that off to other firms.
users. But some are already pointing out terrifying parts of the terms of service that people sign up to use it.

When the headset's software is installed on a computer, it adds a process that allows the PC to watch what the headset is doing and send that back to Oculus. That allows the headset to know when it is being used and turn itself on — but it also allows the company to collect information on people's head movements and activity and send it back to advertisers.

The terms and conditions include a line saying that the headset will collect “Information about your physical movements and dimensions when you use a virtual reality headset”, along with a range of more usual information like data about users' computers and location.

/Gadgets and tech news in pictures
The company lays out some of the ways that it will use the information within the terms, and most of them are mundane. But one line makes clear that Oculus and Facebook will be able to use the information it collects to market to people.

“We use the information we collect to send you promotional messages and content and otherwise market to you on and off our Services,” the terms read. “We also use this information to measure how users respond to our marketing efforts.”

The terms also make clear that the company is allowed to send that data to “related companies” — that includes not only Oculus’s owner, Facebook, but also other parts of Facebook’s “family of services”, like WhatsApp.

More about: | Oculus | Oculus Rift | Facebook
LAW, VIRTUAL REALITY, AND AUGMENTED REALITY
Mark A. Lemley* & Eugene Volokh**

INTRODUCTION

In the summer of 2016, the world suddenly went crazy for Pokemon GO. Millions of people were traveling to spaces public and private to catch, train, and fight with monsters that only they could see. As the mania spread, cities and parks held Pokemon GO parties.1 Hospitals and the Holocaust Museum put up signs warning players that there were no Pokemon to be found on the premises.2 At least one police station politely asked people who came to the police station to catch Pokemon to do so outside the building rather than coming in to bother their officers.3

Gamers and those with a nostalgia for the Pokemon card game loved the Pokemon GO phenomenon. People whose property was invaded by dozens or hundreds of Pokemon GO players hated it, or adapted to it, or tried to make money from it.4 Many other people were puzzled by it. And us? We’re law professors, so naturally our first thought was “just imagine how many potential legal questions this raises!” That’s why lawyers are so much fun at cocktail parties.

Pokemon GO was the first exposure most of the world had to augmented reality (AR). AR allows digital content to be layered over the real world. Using special glasses or, more commonly for now, a smartphone, AR users can see the real world as it actually exists, but with digital images superimposed on the world so that they seem to exist as part of the world. And while gaming is the first application to reach the mass market, it won’t be the last. Our experience of the real

---

* William H. Neukom Professor, Stanford Law School; partner, Durie Tangri LLP. Article © 2017 Mark A. Lemley & Eugene Volokh.

** Gary T. Schwartz Professor of Law, UCLA School of Law; academic affiliate, Mayer Brown LLP.

Thanks to the participants at the UC Davis conference on Future-Proofing Law, the Stanford Law School conference on regulating disruption, and the Internet Law Works in Progress conference for comments on prior drafts; and to Tyler O’Brien and James Yoon for research assistance.


world will increasingly be overlaid with information and images—
sometimes related to what we physically see, sometimes not.

Beyond AR, there is also virtual reality (VR). While AR adds visible
digital content to a person’s perception of the real world, VR replaces
the real world altogether. Using goggles and speakers, VR places people
inside a virtual environment, letting them move around in it and inter-
act with it as if it were the real world.

In some ways, VR is a competitor technology to AR: Business mee-
tings and social interactions with remote parties could happen either via
VR or AR, depending on which technology evolves most quickly. In other
ways, VR can be complementary, with people using AR technology for
adding to physical-world interactions, and VR for creating entirely fic-
tional worlds.

VR also got big in 2016. Four major VR hardware platforms  were
deployed; so were many applications—mostly games, but also immersive
news reporting and social experiments. And the technology, already
impressive in its realism, continues to develop at a breakneck pace.
While most applications of VR today remain games, it won’t be long be-
fore more and more of our interactions occur in virtual rather than real
space (especially as avatars become realistic enough, and begin to reli-
ably track user facial expressions).

AR and VR both present legal questions for courts, companies, and
users. Some are new takes on classic legal questions. People will die us-
ing AR and VR—indeed, some already have. They will injure them-
selves and others. Some will use the technology to threaten or defraud
others.

Sorting out who is responsible will require courts to understand the
technology and how it differs from the world that came before. But it
won’t necessarily require a fundamental rethinking of legal doctrines. A
death threat via AR or VR is legally the same as a death threat via an
oral conversation, a letter, an e-mail, or a fax.

PlayStation VR to debut in October for $399, CNBC, Mar. 16, 2016,
http://www.cnbc.com/2016/03/16/playstation-vr-to-debut-in-october-for-399.html
(PlayStation VR); Signe Brewster, Behind the Numbers of Virtual Reality’s
Sluggish Debut, MIT TECH. REV., Dec. 30, 2016, https://www.technolo-
gyreview.com/s/603208/behind-the-numbers-of-virtual-realities-sluggish-debut/
(Oculus, Sony, and HTC); Darrell Etherington, Google’s Daydream View Made
me a Believer Again in Consumer VR, TECHCRUNCH, Nov. 10, 2016,
https://techcrunch.com/2016/11/10/googles-daydream-view-made-me-a-believer-
again-in-consumer-vr/ (Google Daydream View).

Charles Riley & Yoko Wakatsuki, Pokemon Go-playing truck driver kills

Because VR- and AR-mediated conversations are more likely to be recor-
ed, the VR/AR threat may be easier to prove than an oral threat; but in that re-
spect, the VR/AR threat would be much like a threatening letter.
But AR and VR will also create new legal questions. Virtual interactions will be conducted through devices and networks that are privately owned and operated. Those interactions may therefore be subject to contractual terms and conditions that users will likely never see or consider, but that significantly limit the privacy, property, and liberty rights of those users.

The interactions may not happen in any one physical jurisdiction, and therefore may be harder to regulate effectively. This move—from conducting most of our business in public spaces with public rules, largely located in a single jurisdiction, to private spaces with private rules in which the parties seem next to each other but are really physically in many jurisdictions—may cause us to rethink just what constitutes a legally binding contract and what things we want governed by public rather than private rules.

And AR and VR can also raise other questions that are more fundamental. VR isn’t “real” in the way we normally mean that term. It is an artificial construct, bits cobbled together to produce sounds and images that we observe. But it feels real in a way that is hard to understand until you’ve experienced it. The same may be true with AR, if it can overlay vivid and realistic images of people and objects over the real reality that we see.

This gut feeling of realness can cast doubt on legal doctrines that tend to distinguish between physical contact and physical danger and things that are “just” audio and visual communication. We base many rules on the distinction between the mental and the visceral, between things we perceive and things we experience. VR and AR will make it harder to draw that line, and may push us to think hard about why we punish certain kinds of conduct and not others in the physical world. Indeed, they may even lead us to rethink the notion of what is “real” in a world where more and more of our most significant experiences aren’t “real” in the classic understanding of that term.

VR and AR aren’t the first technologies to challenge legal doctrine. We can, for instance, learn some important lessons from our efforts to apply legal rules to the Internet over the past quarter century. But most of those efforts happened haphazardly, not deliberately. Thinking deeply now about how the law will apply to VR and AR requires us to tread new ground. The reward—hopefully—will be not only a solid framework for applying legal doctrine to some tricky new questions, but also a better understanding of doctrines we take for granted in the physical world.

We begin in Part I, by discussing the rise of VR and AR and how people experience those technologies. We then turn in Part II to how the law is likely to treat “street crimes” in VR—behavior such as disturbing the peace, indecent exposure, deliberately harmful visuals (such as strobe lighting used to provoke seizures in people with epilepsy), and
“virtual groping.” Two key aspects of this, we will argue, are the Bangladesh problem (which will make criminal law very hard to practically enforce) and technologically enabled self-help (which will offer an attractive alternative, but also a further excuse for real-world police departments not to get involved).

In Part III, we turn to tort lawsuits, by users against users, users against VR and AR environment operators, outsiders (such as copyright owners whose works are being copied by users) against users, and outsiders against the environment operators. In Part IV, we discuss users’ alteration of other users’ avatars, or creation of their own avatars that borrow someone else’s name and likeness, and discuss whether that should be viewed as tortious.

We then consider in Part V the likelihood that VR and AR systems will pervasively store all the sensory information that they present to their users (and that they gather in the course of presenting it), and discuss the privacy implications of such data collection and potential disclosure. And we close in Part VI by talking about two overarching issues—order without law and the speech-conduct distinction—that can reflect on broader debates even outside VR and AR.

Our article primarily aims to identify the interesting coming questions, and outline some possible answers. We will sometimes suggest which answers are best, but that’s not the main value that we seek to add. Rather, we simply hope that, by thinking ahead about such matters, all of us can better decide how to better develop both VR and AR law and VR and AR technology, and perhaps also learn something about the role of law in the physical world as well.

I. THE RISE OF THE MACHINES

A. The technological background

How did 2016 come to be the year of VR and AR? From a technical perspective, the success of AR and the ability to start deploying VR stem from several trends coming together.

First, computer processing power continues to grow exponentially, roughly following Moore’s Law. That permits real-time processing of enormous amounts of data on ever-smaller devices. It also permits highly realistic graphics, as anyone who has played a modern computer game can attest.

Critical to VR, what was impossible with even a cluster of super-computers a decade ago—real-time rendering of a world that surrounds you and responds as you interact with it—can now be done on a home PC and deployed to a lightweight, fairly comfortable headset. Indeed, lower-quality VR images without interactivity but with full surround

---

8 See https://en.wikipedia.org/wiki/Moore’s_law.
video are already being sent to your smartphone with a headset made of cardboard.\textsuperscript{9} For the moment, the best VR experiences require a cable connected to your PC, but that’s likely to change soon, as on-board headset processing power and wireless communications technology improve.\textsuperscript{10}

AR takes advantage of the same technological developments, but also some additional ones. First, likely about two billion people in the world now have in their pockets a computing device of incredible power.\textsuperscript{11} Second, wireless connectivity lets that device connect to the Internet and other devices in almost all populated places in the world. Third, those devices come with very good built-in location tracking services. Those factors put together mean that you can send graphics and other information to a phone or other portable electronic device and know where that phone is and where it’s looking when you do.

AR and VR also differ in the openness of the technologies they employ. If you play Pokemon GO, the monsters you see on your screen are provided by the game maker, Niantic. But the screen on which they appear is your smartphone. The game can be played on any phone platform, and players with iPhones can see and interact with players with Android phones. AR is, at least generally, interoperable.

VR, by contrast, is not. VR is currently the province of a variety of proprietary headsets, such as the Oculus Rift, the Vive, the Playstation VR, and the HoloLens. Each platform runs its own games, sometimes on different computer hardware. While we expect that more games and apps will be written to work on multiple platforms over time, for the foreseeable future those programs will not work across platform. If I want to interact with a friend in a VR game or business meeting, we both have to wear the same type of headset.

\subsection*{B. The practical applications}

So far, most uses of VR and AR have been in gaming. Pokemon GO is a good example of AR using phones plus location plus graphics processing to generate images that are superimposed on the real world, allowing players to go to real places to find and capture virtual monsters. VR gaming offers far more exciting prospects, because it takes the user

\begin{thebibliography}{9}
\end{thebibliography}
into the game itself. Rather than controlling an avatar on a screen, the user becomes the avatar, and the physical movements of her body translate into the world she perceives around her. Even at this early stage, the effects of the technology can be remarkable.

Some readers may be inclined to dismiss VR and AR as unimportant because they are “just” gaming platforms. That would be a mistake. First, gaming itself is an enormous and underappreciated business and social phenomenon. Gaming is a significant phenomenon worth studying in its own right, and likely to become more so over time, since it is growing far faster than other forms of media. About 25 million Americans identify themselves as active video gamers. The industry is a $30 billion annual business in the U.S., and $90 billion worldwide. It has spawned its own popular television network, Twitch tv, and in 2015 more people tuned in to watch the finals of a League of Legends tournament than watched the NBA basketball finals.

And VR also changes the way people react to games. Kids playing violent VR videogames, for example, have higher physiological arousal and aggressive thoughts than those observing someone play the game on a 2D screen.

But the use and promise of AR and VR are also not limited to gaming. Google’s entry-level phone-based VR app, Cardboard, launched with immersive video news reporting, allowing you to visit Syria and other news hot spots around the world, looking around (though not interacting). VR programs like Tiltbrush are already letting artists create art in three dimensions by working inside their creations. VR art has al-

15 Sandra Calvert & Siu-Lan Tan, Impact of Virtual Reality on Young Adults’ Physiological Arousal and Aggressive Thoughts: Interaction Versus Observation, 15 J. APPLIED DEVELOPMENTAL PSYCH. 125 (1994).
ready appeared in major museums. VR systems will allow a new generation of computer-aided design of products.

Other VR projects have included diversity training that lets people change their race or sex and see how others interact with them when they look different than they do outside VR. VR will also doubtless be used for training people for various physical tasks; think airplane simulators, but for activities that have much more complicated and dynamic controls.

AR is technically quite interesting, and will become even more so when it moves from cell phones to glasses. The first well-known attempt, Google Glass, proved to be a failure. But we think that is a problem with this particular implementation. The technology, when implemented right, will be powerful and profoundly appealing, not just in gaming but at work and in social life. AR apps include not only gaming, but the ability to superimpose relevant data over an image on a computer screen. Google Glass offered a computer screen that projected information over a real view of the world. Other AR projects includes heads-up displays for pilots and drivers that let them access important information without looking away from the road or the runway.

AR glasses can help workers in their jobs, by pointing out extra information about the objects they are manipulating, or alerting them to safety risks. They can help people professionally by giving them instant access to information they may need for their negotiations or other business conversations. Most relevant to what we’ll be discussing below, they can help people interact with coworkers, business partners, friends, and family who are not physically present, by projecting the other person’s image into the wearer’s field of view. Coupled with high quality audio, such video presence can create much more lifelike interactions than currently available with Skype and similar videoconferencing systems. Implemented well enough, it can save billions of dollars in business travel costs (especially considering the cost of traveler time as

\[18\] Id.


\[20\] Marco della Cava, Virtual Reality Tested by NFL as Tool to Confront Racism, Sexism, USA TODAY, April 8, 2016.


\[23\] Hayley Tsukayama, Everything You Need to Know About Google Glass, WASH. POST, Feb. 27, 2014.

well as of transportation and hotels). And it can help people maintain friendships and family life across distance.

And there is much more coming. The ability to overlay data on an image of the real world (or, with Glass, on the real world itself) has myriad possible uses beyond depicting cute monsters. Imagine that you walk into a cocktail party and someone who looks vaguely familiar comes up to say hello to you. AR offers the possibility that your glasses could run facial recognition software, identify the person, and unobtrusively tell you who they are (and remind you of the names of their spouse and kids, and the last time you saw each other).

VR and AR also offer the possibility of real-time interaction with people from around the world—not just text chat, or even video conferencing, but actual interaction. Interacting in a virtual space lets people behave naturally in a way that a phone or computer screen will not permit. It also allows collaborative design of art, architecture, or virtually anything else.

And then, inevitably with new technologies, there is sex. Realistic, interactive pornography—whether with live remote participants or with software constructs—is likely to drive a significant amount of early VR business, and also to push technical development in VR towards more realistic avatars. That will be important for reasons we discuss in Part IV. And the development of sexual “haptics,” devices that can reproduce sensations and not just sights and sounds, will take things far beyond mere pornography.

C. The effect on our interaction with the world

1. Distraction

VR and AR will not simply offer new ways for us to interact with each other (or to interact with constructed worlds with or without each other). Based on what we know from existing VR and AR, both technologies will affect the way people interact with the world around them.

Consider the distracting tendency of AR. It is no surprise that people find cell phones distracting. Traffic deaths are up after years of decline, in large part because people are texting and driving. Phones

---


are attractive nuisances, and we are generally less good than we think we are at splitting our attention between them and the real world.

But if a normal cell phone screen is distracting, AR has the potential to be especially so. While some AR implementations—such as heads-up displays—are designed to minimize distraction,28 the temptation to just look for a moment at the latest alert is almost irresistible. That temptation becomes even stronger when the alert doesn’t signal you from your hand or your pocket but actually overlays what you see with your full field of vision. There are already instances in which people playing Pokemon GO have walked off a cliff or into oncoming traffic.29 And the distractions of AR are only likely to increase with time.

2. Immersion

If we react to AR by splitting our attention (badly) between the world around us and the virtual world layered on top of it, we react to VR by ignoring the real world entirely in favor of the world we experience inside the headset. If you haven’t experienced true immersive VR for yourself, you might find it hard to believe just how real it feels inside the headset. But one experiment may give some perspective.

In one VR application, you can walk out onto what appears to be a board high in the air and jump off. You are not, of course, standing high above the ground. Your mind knows this, because a minute ago you were standing in a flat room, because there are people standing right next to you talking to you, and because you know you are in a VR experience.

Nonetheless, a large proportion of the people in this simulation won’t even walk out onto the board because it looks precarious. Some panic and have to take the headset off altogether. Of those who do walk out, most aren’t willing to step off the “plank” and (presumably) fall, even though the step is in reality only a single step on a flat surface in a normal room. And even those who do step off—who presumably let their intellectual awareness of their physical surroundings control what their senses are telling them—invariably lean forward and start to fall as they take that one step, because their body is signaling them that they are falling.30

There are many more examples of the very real feeling we get when we are in VR. We experience what happens there as if it were really


30 Liat Clark, Walking the Plank with the Oculus Rift is Stomach-churning stuff, WIRED, May 30, 2013.
happening, whether it is a close encounter with a whale, or enemies jumping out to take shots at us.

One study used VR to replicate the Milgram shock experiment—a famous psychology experiment in which a subject is asked to press a button to electrically shock a stranger in another room. There are no actual shocks delivered with the button, but during the experiment, the stranger cries out in pain and the subject hears those cries.

In the original Milgram experiment the test subjects thought they were administering real electric shocks to real people.31 Not so in this experiment. In spite of the fact that all participants in the VR study knew that neither the stranger nor the shocks were real, the “participants tended to respond to the situation at the subjective, behavioural and physiological levels [as measured by skin conductance and heart rate] as if it were real.”32 Those subjects who interacted with the stranger via text screen did not produce comparable levels.33

Many people cannot separate their intellectual understanding of what is happening from the very different signals their body is sending them. And even for those who can, the body will not be ignored. It releases chemicals in response to perceived threats, pleasures, or opportunities whether or not the brain knows those things aren’t real.

People in VR environments physiologically respond to actions done to them in VR.34 Subjects who see themselves getting slapped in VR respond with skin conductance and heart rate levels as if they were actually getting slapped. The results are replicable even when the subject is male and their VR “body” is female.35

Indeed, the realism of VR can be harnessed for therapy. VR has been effectively used to treat stress36 and brain damage37 because the

---

32 Mel Slater et al., A virtual reprise of the Stanley Milgram obedience experiments, 1 PLoS ONE e39 (2006); Marcus Cheetham et al., Virtual Milgram: empathic concern or personal distress? Evidence from functional MRI and dispositional measures, 3 FRONTIERS HUMAN NEUROSCIENCE 29 (2009).
33 Slater, supra note 32.
34 Mel Slater et al., First person experience of body transfer in virtual reality, 5 PLoS ONE e10564 (2010).
35 Id.
36 Matilda Annerstedt et al., Inducing physiological stress recovery with sounds of nature in a virtual reality forest—Results from a pilot study, 118 Physiology & Behavior 240 (2013); Youssef Shiban et al., Trier Social Stress Test in vivo and in virtual reality: Dissociation of response domains, 110 INT’L J. PSYCHOPHYSIOLOGY 47 (2016).
human nervous system responds to stimuli in VR environments similarly to ones in the physical environment. Several studies have particularly focused on the treatment of anxiety disorders through exposure therapy in VR; though overall anxiety was lower in VR environments, the magnitude of anxiety decline in the VR treatment and real-world treatment was similar.38

VR therapy has also been compared to imaginal therapy—asking patients to imagine the anxiety-inducing situations. Patients in VR therapy exhibited more anxiety during therapy but a greater decline in anxiety as a result of therapy than did patients in imaginal therapy.39 VR made the experience seem more real.

VR is, in a word, a visceral experience. Things that happen there aren’t physically real: If the bad guy shoots you in Bullet Train, you don’t die in real life. But they feel very real indeed.

And those feelings can in turn have real physical consequences. You could literally be scared to death (or at least into a heart attack) by a game that felt sufficiently real. Even if you aren’t physically harmed, you will have experienced what you saw and did in VR in a way that you do not on the Internet or in a normal video game. And that fact has significant consequences for how the law intersects with VR, as we will see in the next Part.

3. Image

VR and AR, when they show us to others, don’t show us as we actually appear. Capturing our actual appearance in 3D, transmitting this video, and superimposing it on the receiver’s VR environment is too difficult even for modern technology. (It requires not just extra bandwidth, but many cameras surrounding us.) Instead, we appear through our avatars. Today, the avatars look cartoonish, but they will become increas-


ing realistic-looking, and will include our facial expressions, which will be captured in real time and superimposed on the avatar. 40

But realistic-looking need not mean real. They could, for instance, be nicely dressed and coiffed versions of us, even if when we’re actually looking into VR in our pajamas before our morning shower. Naturally, they could be somewhat younger and better-looking versions of us. Or if we’re young but want to seem more mature in business interactions, we can use slightly older-looking avatars. In any event, we will look like we want ourselves to look, no longer bound by the limitations of our actual appearance (except insofar as social or business conventions might treat sharp departures from our real appearance as untrustworthy or manipulative).

Indeed, avatars could be largely or entirely disconnected from our real appearance: of a different sex, of a different race, with different facial features, lacking our disabilities. Or they could look like dinosaurs. This could be done for experimentation, for pseudonymity, or to avoid hostility.

This malleability of visual identity has minuses as well as pluses. Easy pseudonymity could mean less social accountability (just as physical distance may mean less legal accountability—more on that later). People could also feel professionally or socially pressured to take on personas that seem inauthentic to them, but that seem more profitable. This may be true with regard to race and sex, but it will be even more true of avoiding physical features that our society views as ugly or off-putting.

At the same time, many people are likely to be quite enthusiastic about the possibility of beauty—or just being aesthetically average—coming at next to no cost and next to no investment of time. Many women spend hours each week on makeup and hair for work; that may be a regrettable demand of our culture, but it’s quite real. If they can instead VR- and AR-commute, all that time will be saved. More importantly, many people who are self-conscious about their appearance can be freed from that. Many who find themselves treated worse because they are obese or otherwise socially stigmatized will be able to avoid that.

And of course, as with much modern technology, VR and AR will be especially useful for people who are physically disabled—not just because they could conceal their disabilities, if they want that sort of privacy, but because they could often much more easily “get around” in VR and AR than they could in the physical world. It’s not clear to us how much all this will affect law as such, but it will certainly affect people’s experience of the technology. (Returning to a point mentioned in the

previous section, it will especially affect people’s online sex lives; but appearance unfortunately matters in business and socializing as well.)

Indeed, the ability to obscure aspects of one’s identity has proven socially useful in other contexts. The percentage of women who won jobs in orchestras went up dramatically after orchestras began blind auditions in which the interviewers didn’t know the race or gender of the person performing.41

VR offers the same possibility for job interviews. We may be able to significantly reduce subconscious race and gender bias in interviewing (as well as bias against fat, bald, or ugly people) if the interviewers see an avatar who doesn’t look like the real person. On the other hand, to the extent that the VR software lets one modify the facial expressions that one is sending, that could hide potentially valuable visual cues related to how much attention the interviewee is paying, how much attention he is showing, and the like.

4. Data

The reality you feel in VR is made out of bits, of data. And because it is, it is owned and stored somewhere by a private company—or perhaps several. Those private companies will invariably impose terms of use that purport to bind users of the hardware and software. Those terms may disclaim liability for harm. They may assert ownership over the things we create in VR. And they may require us to consent to having information about our conduct in the virtual world recorded and shared.

Our movements and actions in the physical world are increasingly observed, recorded, and tracked. But there are still spaces where we are not followed and acts that are not recorded and searchable. In VR that will likely not be true. Everything we do, we do before an audience—a private company that may well keep and catalog that data, and may have lots of reasons to do so (data mining, security, user convenience, and more).

Of course, the same is true of the Internet today. But we may do, say, and experience things in VR we would not put in an email. That VR feels like the real world may cause us to treat it like the real world. When we feel like we are alone with someone, we may be more likely to share intimate secrets than we would on a public street, or even in an email. But in VR those secrets are, inevitably, being recorded somewhere, and are likely being retained.

II. CRIME ON THE VIRTUAL STREET

That, then, is the likely technical and social reality of VR and AR. What legal problems will it cause? Let us begin with the VR and AR equivalents of street crimes.

A. What would VR/AR street crimes be like?

Much traditional criminal law enforcement involves street crimes: in-person misconduct, such as robbery, sexual assault, indecent exposure, or disorderly conduct. Many such crimes literally happen on the street. Many others happen in homes, businesses, or schools, but share many traits with traditional street crimes.

Many of the worst such crimes aren't a problem in VR. You generally needn't worry about being really murdered in a virtual space. Likewise, you needn't worry (subject to some complexities that we'll mention below) about being really beaten or raped.

Indeed, this could be one reason people will shift some activities to VR. Physically going out to drink with friends might be more fun in some ways than getting a virtual drink, where everyone is physically at home but can see each other in VR. You can hug your friends in a real bar. You can feel physically close to them and not just emotionally close. If you're looking to pick up a sex partner for the evening, doing that in VR would require haptic hardware that goes beyond what we have today.42

Yet going out together for a virtual drink—to be precise, staying in for a drink, but being virtually together—has its own advantages. You needn't worry about getting into a bar fight, or getting mugged on the way home. You needn't worry about driving home drunk, or paying for a cab. Plus, the booze is much cheaper at home.43

Still, as we'll discuss below, there may well be some kinds of “street crime” in VR. How will the law likely deal with that? How should it?

1. Disturbing the peace and the Bangladesh Problem

What sorts of street crime can there even be in VR? Today's VR is basically audiovisual—you can see and be seen and hear and be heard, but you can't be punched or shot or caressed. (Caressed is surely on its way, but not here yet.44) We thus focus on crimes of sound or of sight.

42 Of course, people are working on changing this. See, e.g., Alex Hawgood, ‘Interactive’ Gets a New Meaning, N.Y. TIMES, Dec. 24, 2013.
43 A drinkable $15 750-ml bottle of hard liquor contains about 15 shots' worth (assuming each shot is 50 ml, or about 1.75 fl oz), so that amounts to $1 per shot. Your VR headset can pay for itself so quickly.
44 See supra note 42.
A classic sound crime is disturbing the peace through loud noise, for instance through screamingly loudly in a public place.\textsuperscript{45} That crime can pose First Amendment problems when applied to speech that disturbs because of its content,\textsuperscript{46} but it's pretty straightforward when applied to speech that disturbs because it's too loud.\textsuperscript{47}

Indeed, if you see someone standing on the sidewalk screaming, calling the police is a standard response. You expect the police to come out, maybe talk the guy into going away, maybe arrest him, maybe even have him prosecuted. Dealing with such annoying street behavior is part of what police normally do.

Now say someone is screaming in a VR public place. Let's assume this isn't in a game, but in a place where people need to congregate for economic reasons—to shop at a VR store, or even go to their VR jobs. The harm caused by the screaming is the same: It interferes with people's other tasks.

So you call the police.

“Officer, there's this guy screaming and bothering my kids and me.”

“What's the street address?”

“It’s not on the street, it's in this VR world.”

[Pause.]

“We're playing a virtual game in the virtual park, and this guy is bothering us.”

“Where are you, really?”

“Well, I'm sitting in my bedroom, but that's not what's important! I'm wearing my virtual headset, and it feels to me like I'm playing with my kids in the park—they're with my ex across the country, but we're spending some time together, and this jackass is ruining it for us.”

“And where is he, really?”

“Oh, I clicked on his avatar, and it tells me that he's hooked up from Dhaka—you know, in Bangladesh. But it feels like he's right next to us.”

[Click.]

Now maybe if you call a more technically savvy police agency, they'll understand your concerns more quickly. But their reaction is likely to continue to be skeptical, because of what we label the "Bangladesh problem": It will take a lot to get domestic police interested in investigating


\textsuperscript{46} \textit{E.g.}, Cohen v. California, 403 U.S. 15 (1971).

\textsuperscript{47} See, e.g., Kovacs v. Cooper, 336 U.S. 77, 82–83 (1949).
a crime where the criminal is in a foreign country. Indeed, it will take a lot even if the criminal is in another American state, or perhaps even in another city. Getting some extradited is a hassle. Even dealing with another jurisdiction’s police department to arrange an arrest in the same state is a hassle.

Will they go through the hassle to investigate a murder? Maybe. But, “You think I can get someone extradited from Bangladesh for disturbing the peace?,” the police officer might ask you. “Or even from Nebraska?” Indeed, perhaps your state won’t even have jurisdiction over such crimes committed by people screaming in their rooms elsewhere in the world; but even if the state is legally entitled to prosecute such crimes, it would surely be very hard for local police and prosecutors to bring such a prosecution.

And there’s every reason to think that the VR street criminals would indeed live all over the world. There are no oceans or borders in VR—that is one of its advantages. The VR “places” in which Americans will travel will be disproportionately Anglophone (though good real-time translation might change that), and disproportionately drawn from richer countries. Yet many of the people who share the same VR “street” will be oceans apart, and most will at least be from different states.

The same problem already exists to a significant extent on the Internet. The people who harass you or even threaten you on Twitter or Reddit, can as easily be in South Africa as in South Carolina. Courts handling civil cases have struggled for decades with how to address the problem of people who cause injury far from where they live. But criminal prosecutions for such transnational threats appear to be vanishingly rare.

Yet the illusion of presence that VR and AR bring is likely to make potentially criminal incidents more common. It’s relatively rare for someone in a foreign country to care so much about us that he would tweet death threats about us; it happens, but only for pretty high-profile people. Most threats seem likely to stem from personal, emotionally laden interactions that usually require a sense of in-person connection—people threatening their exes, gang members, schools, and the like.

But the crimes we describe in this subsection and the coming ones are likely to be much more common. People scream and create a public

48 We have nothing against Bangladesh: It’s just a good example of a populous country that is very far away, that contains millions of English speakers, that likely won’t make it trivially easy to extradite petty offenders, and that has a fun polysyllabic name. Use “South Africa problem” or “India problem,” if you prefer.

49 Alec Ross, The Language Barrier Is About to Fall, WALL ST. J., Jan. 29, 2016.

commotion in the real world; there’s no reason why they wouldn’t do the same in a VR space. People indecently expose themselves in the real world; there’s no reason why they wouldn’t do the same in VR (more on that below). Indeed, they may be more likely to do this, precisely because they may reasonably infer that it will be hard for the police to catch them. Moreover, there will be more desire for criminal prosecution than with Internet misconduct, precisely because the feeling of physical presence may make the victims of VR street crime viscerally feel victimized. That desire, though, may be hard to satisfy.

To be sure, VR does tend to facilitate policing in one way, by solving some problems of proof and identification. If the VR platform keeps good logs, it can accurately report just which avatar was screaming, and just how loud he was. And perhaps the VR platform requires people to identify themselves before accessing it, at least with a credit card; or with the proper subpoenas, the typical avatar can be traced back to an Internet subscriber. But the greater difficulties caused by extradition are likely to exceed the greater ease of proof. And many VR street crimes might thus be practically ignored by traditional police department.

Of course, this might yield pressure for VR operators to set up in-VR “police,” who might be able to deal with transgressors quickly; and there might be “courts” as well, for resolving disputes (especially disputes involving in-VR commerce). But the penalties will likely be, at most, suspension or ejection from the VR environment. And it seems likely that the ejected participants can just get back on by creating a new user ID.

If a VR environment requires people to provide a credit card, or otherwise supply a deposit, such new user IDs might become harder to create, and the environment might even threaten fines or forfeited deposits for bad behavior. How often this will happen will depend on economic factors that we can’t easily predict. We expect that many VR environments will want to allow free access, or at least access that doesn’t require a credit card (but might require only some prepaid gift card), since the VR operators will want to harness network effects by increasing their user bases. Presumably, those operators will make money from in-VR purchases rather than through credit card subscriptions. But we’re not certain whether this will be so; indeed, some environments might want to require credit cards or elaborate identification systems precisely to maintain a more orderly experience for their users.

So the real-world police are unlikely to intervene to stop the VR street screamer. But there’s a good reason why disturbing the peace is a crime: It affects people’s quality of life, and tends to push them away from a place where they want to be, and where we might want them to be (for instance, if we want them to work there or shop there). And the creators of the VR environment will be keenly aware of this, because lost quality of VR life means lost profits to them, especially since different VR environments will likely be hotly competing with each other.
Code, as Larry Lessig put it, is law—maybe the most effective sort of law.51 And VR environment operators can easily implement code that can deal with the screamers. The operator could, for instance, allow each user to control the perceived volume, for that user, of any other user. That’s good not just to silence the screamers, but also to quiet down acquaintances who are a bit too loud, or to amplify acquaintances who matter. And this should be technically trivial to code.52

The instruments of the real world—real ears and real brains—don’t have such a feature. But the sensescape created by the VR software is more versatile and more individually controllable than what mere human anatomy can provide.53 Taking advantage of this versatility can help prevent or quickly interrupt VR street crime. Yet shifting to these in-VR remedies likely means shifting away from the criminal law, and from the standard criminal law penalties.

2. Indecent exposure

We can see the same if we consider another crime, this one visual rather than aural: indecent exposure.

There you are, minding your own VR or AR business, and you see this avatar a few feet away from you—and he’s naked. Plus he’s unusually well-equipped; if you’re going to have an avatar, why settle for mere realism? Or maybe he’s naked and deliberately grotesque. (Two penises?) Or maybe he’s masturbating. Or having sex with someone.

You avert your eyes, but he pops right in front of you, wherever you look. And this might happen even when you aren’t practically able to leave—for instance, if your in-VR job requires you to be “present” in that particular VR “location.”

If this were happening on a street, the exhibitionist would probably be arrested for indecent exposure or public lewdness.54 But whether this law can be applied in VR turns out to be surprisingly complicated.

51 LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).
52 AltSpaceVR, a prominent program for social interaction in VR, already has such a feature. AltSpaceVR, How Do I File an Abuse Report?, Mar. 1, 2017, https://help.altvr.com/hc/en-us/articles/206865083-How-do-I-file-an-Abuse-Report (“Before you submit [an abuse] report, we suggest Muting the individual that is being a disturbance. You can click the ‘Mute’ button on their nametag. This will cause them to stop moving and will eliminate any audio that they may be producing through their microphone.”).
53 By “sensescape,” we simply mean the array of sensory inputs that a VR environments provides to users: today, mostly sights and sounds, but it could soon include touch, smell, temperature, pain, and more. Riley Snyder, Getting Physical with Virtual Reality, L.A. TIMES, Jul. 18, 2014.
54 He might also be deterred by social convention, or perhaps by the sense that he doesn’t look that good naked. But in VR, he can look as good (or as grotesque) as he wants, and he doesn’t have to show his real face. There may be
The Supreme Court has held that public nudity may be banned even in strip clubs, where the patrons pay money to see such nudity. But the Court has also held that the First Amendment protects public displays of films containing nudity, even on drive-in theater screens visible from the street, where unwilling drivers and pedestrians may see the nudity (moving, in color, twenty feet high).

Even outside VR, this can be confusing enough that a Michigan appellate court has upheld an indecent exposure conviction for a man’s displaying his penis on a public access cable television show that he produced. This seems inconsistent with the drive-in case, but it may just reflect a deeper inconsistency between the drive-in case and the public nudity cases.

This gets even more complex when we go beyond video of nudity to video of sexual behavior. If the video is obscene, then it can theoretically be punished even when the viewers are consenting. And even material that is not outright obscene enough but is nonetheless “obscene-as-to-minors” might still be punishable when it is deliberately shown in public places where minors may be present. But the Court has held that the government can’t ban such obscene-as-to-minors material online, even in places that minors can access, because a less restrictive alternative is to have parents use filtering software to shield their children, if they so wish.

Perhaps the drive-in case and the public nudity case, though, can be reconciled: Public nudity is viscerally perceived as real and immediate in a way that a video display is not, the theory would go; and public nudity thus evokes reactions from which the law can legitimately protect people.

immediate and temporary social sanctions—for instance, if he goes naked into a VR shop, he might get ejected—but then he can just quickly change his avatar to something clothed, and then change it back when he’s done shopping.

58 One of us filed an amicus brief in Huffman supporting review by the Michigan Supreme Court, but that court denied an appeal, by a 5-2 vote. People v. Huffman, 708 N.W.2d 95 (Mich. 2006).
60 See Crawford v. Lungren, 96 F.3d 380 (9th Cir 1996) (upholding ban on unattended coin-operated newsrack sales of “harmful to minors” material); American Booksellers v Webb, 919 F.2d 1493 (11th Cir. 1990) (upholding ban on display, in a place accessible to minors, of any material that’s “harmful to minors”); Davis-Kidd Booksellers, Inc. v McWherter, 866 S.W.2d 520 (Tenn. 1993) (same).
If that’s so, public nudity in VR and AR becomes a harder case. After all, nudity in VR is technically display of video (as in the drive-in case) but also functionally aimed at emulating in-person presence (as in the public nudity cases). And while the avatars so far are relatively cartoonish, it won’t be long before a nude VR avatar—normal size, with normal movements, seemingly standing next to you—feels a lot more like a physically present person than it does like a picture on a screen.

One reason the law forbids indecent exposure is that such public nudity may lead some observers to worry that the exposers may move on to sexual assault.\(^{62}\) That is a serious worry when the exposers are physically nearby, but not when the exposers are present only virtually. Nonetheless, unwanted exposure to others’ nudity may cause feelings of unease even when it is logically clear that no in-person assaults are possible. So whether we should be more worried about indecent exposure in VR may depend on whether we think the primary focus of the law is on the unease that it creates among passersby, or on public indecency as a proxy for future physical attack.

But maybe this legal conundrum is likely to stay academic. First, we’re back to the Bangladesh Problem. How many police departments would relish the prospect of trying to extradite someone from a foreign country, or even another state, because his online avatar is nude?\(^{63}\)

Second, as with loud avatars, VR users may be able to protect themselves from unwanted nudity in many circumstances. VR environments can easily be designed to let users change how others’ avatars appear to them. “My avatar,” after all, is just a visual image that I would like to present in displays that come up on others’ VR goggles, communicated through the VR software on central computers and on other users’ computers. Those users don’t have to perceive me as the avatar I chose.\(^{63}\)

They could, for instance, substitute another avatar; if my avatar is Adolf Hitler and they don’t like it, they could substitute Mahatma Gandhi (or vice versa). Or they could just edit the avatar: If my avatar is naked and they don’t like it, they could color it solid green, or perhaps solid green except the face (software permitting, but this should be easy software to develop). Conversely, if they’d like to see more nudity, they could replace my avatar with whatever naked version—they prefer.\(^{64}\)

---


\(^{63}\) Allowing that sort of modification may create other legal problems, however, as we discuss below.

\(^{64}\) The VR operator might also let the VR store outside which the nude avatar—or the screamer—is standing exercise some control over such behavior.
Indeed, they could probably use a program that automatically blacks out all the naked parts of naked-seeming avatars.65 Or the operator can require people who select a nude avatar to also provide a nonnude version, so that people who prefer to avoid seeing nudity can select that with just one global switch. This might be useful if the automated editing yields results that are too crude to yield an enjoyable VR experience, or if the operator wants to minimize even the initial unwilling exposures to nudity.66

Now let’s play out again a conversation with the police, focusing on how this technologically enabled self-help might affect their decision.

“There’s this avatar standing in the VR park, and he’s completely naked!”

“Why don’t you just hit the ‘dress up the avatar’ button?,” the police officer asks. (Again, we assume an officer who knows something about VR.)

“I shouldn’t have to do that!,” you say. “He’s violating the law, and it isn’t up to me, the victim, to try to avoid that.”

And that’s a plausible argument, in theory; as you point out to the officer, “After all, ‘To say that one may avoid further offense by turning off the radio when he hears indecent language is like saying that the remedy for an assault is to run away after the first blow. One may hang up on an indecent phone call, but that option does not give the caller a constitutional immunity or avoid a harm that has already taken place.’ Justice Stevens said that, you know. In FCC v. Pacifica.67 Same for nudity as for vulgar language.”

But our police officer is not a theorist. “Are you telling me that you could have avoided this problem by clicking on a button,” he says, “and you’re bothering me? I have real crimes to deal with—ones in which the victims really need me to do something that they can’t do for themselves.”


66 Presumably the operator would enforce this by threatening to delete nude avatars that lack a nonnude version and that yield complaints, and perhaps to delete the offending users’ accounts and make it a hassle for them to create new ones. This won’t stop the determined repeat offender, but given that it’s easy enough to create both a nude and nonnude avatar, most users would likely choose to comply with the operator’s policy rather than go to the trouble of repeatedly evading it.

Or, if the officer is a theorist, perhaps he is one of the economic rather than deontological variety. “You are the cheapest cost avoider here,” he says. “You can avoid the unwanted nudity with just a few clicks, whereas I would have to go through much more effort to prosecute it. I know that the criminal law does not usually formally focus on that; but, practically, it makes me reluctant to give your call a high priority.”

Now of course there are limits to this “you should have avoided the problem yourself” argument. Presumably if the crime is more serious—say, burglary—the police wouldn’t just say “your own fault for having left your front door unlocked, we won’t investigate the case.” But for minor enough crimes, and ones where the main worry is prevention going forward, the police are unlikely to invest many resources into such prevention when citizens can more effectively prevent the problem themselves.

And this tendency only increases as a result of the Bangladesh Problem. As arrest and prosecution becomes much more expensive for the police, and technologically enabled self-protection simultaneously becomes less expensive for citizens, the police are likely to become less interested in intervening, especially in cases that don’t seem to them to involve any “real” harm.

3. Strobe lighting

Here’s a possible test case that does involve a serious harm that is harder to avoid: About 3% of people who have epilepsy—disproportionately, young people—can have seizures triggered by strobe lighting.68 Though such seizures tend not to be fatal, or even greatly injurious, at least when the person having the seizure is just sitting in his home in front of his computer, they do involve a nontrivial risk of injury. This hasn’t been seen as reason enough to generally ban strobe lights, especially since such lights seem to be entertaining for many people, and are sometimes used as a safety feature.69 But deliberately creating a strobe effect in VR precisely to play a nasty prank on someone you know to be endangered by this would likely be tortious or even criminal.70

68 About 1% of the population has epilepsy, Rosemarie Kobau et al., Epilepsy in adults and access to care—United States 2012, Morbidity and Mortality Weekly Rep. 909, 910, so this 3% of 1% amounts to about 100,000 people in the U.S., and many more outside.


But here, too, a program running on a user’s VR headset might be able to detect strobe lighting and convert it to something nonstrobing. People who know they are strobe-sensitive, or who even think they might be, could then easily turn on this program.71

The initial exposure—for those who have neglected to get and turn on such a program, or for those who are unaware that they need it—is materially more dangerous than in the disturbing the peace scenario: physical injury, and not just annoyance. And an attempt to deliberately trigger a seizure, as in our hypothetical, is highly morally culpable. The purpose is to harm someone, even if most of the time the purpose will be frustrated by the targets’ precautions.

Would this be enough to lead the police to be willing to intervene? Or would they likely not think this to be worth triggering a possible interstate or international investigation, when, at least going forward, the victim could avoid such harms through technological means?

The strobe light example is the rare virtual hypothetical that combines such culpability with the real risk of physical injury, but others might arise in the future: Imagine, for instance, a hack that alters the VR camera positioning information so that a user who thinks she is in the middle of her living room is in fact standing at the edge of the stairs, or that deliberately sends someone using AR walking into a wall or off a cliff. The use of VR (or, more likely, AR) systems to deliberately cause physical harm to a user is more likely to get the attention of police and courts than are disturbing the virtual peace or virtual indecent exposure. But it will do so precisely because the consequences are more obviously physical rather than virtual.

4. “Virtual groping”

Harm, though, can also feel real without being physical. Only a few months after commercial VR became available, a woman named Jordan Belamire (a pseudonym) was “virtually groped.” Belamire recounted playing a multi-player zombie shooter game when another player—who recognized Belamire as female by her voice—began to make gestures that seemed like virtual groping:

In between a wave of zombies and demons to shoot down, I was hanging out next to BigBro442 [the other player], waiting for our next attack. Suddenly, BigBro442’s disembodied helmet faced me dead-on.

71 For a pre-VR analysis of this, see How Is TV Made Safe for People with Epilepsy?, BBC, June 7, 2007; see also Univ. of Md. College of Info. Studies, Trace es. & Dev. Ctr., Photosensitive Epilepsy Analysis Tool, https://trace.umd.edu/peat (offering a free program that will analyze whether a video poses an epilepsy seizure risk, and that could likely be easily adapted to provide real-time filtering of dangerous strobing).
His floating hand approached my body, and he started to virtually rub my chest. . . .

[Even when I turned away from him, he chased me around, making grabbing and pinching motions near my chest. Emboldened, he even shoved his hand toward my virtual crotch and began rubbing. . . .]

And Belamire reports that BigBro442’s behavior, though utterly lacking in physical contact, seemed so realistic as to be disturbing. Belamire had earlier in her article described how realistic a VR cliff seemed to be, triggering her fear of heights.73

“The virtual groping,” she said, “feels just as real. Of course, you’re not physically being touched, just like you’re not actually one hundred feet off the ground, but it’s still scary as hell.” Her experience is consistent with the studies we reported in Part I.C.2 suggesting that people react physiologically to touches in VR much as if they had happened in the physical world.

Under current law, virtual groping probably wouldn’t be a crime. It isn’t sexual battery, because there’s no touching.74 Tort law tends to define “assault” as including an actor’s intentionally putting someone in “imminent apprehension” of “offensive contact,”75 but criminal law tends not to outlaw such behavior unless it is actually an attempt to commit battery.76 And beyond that, it’s not clear that such imminent apprehension would be present when the target consciously knows that no physical contact is possible. While sexual threats by remote actors over the Internet have sometimes been treated as crimes, those cases all hinge on the plausibility that the threat made over the Internet will be carried out in the physical world.77

Should the law be changed? We suspect that very few people would find virtual groping, accomplished through purely visual means, to be as upsetting as real groping. Nonetheless, Belamire is doubtless right that, because of the visceral feeling created by virtual reality, such virtual


73 This is similar to the plank experiment, in which many VR participants find it very hard to step off what looks like a plank over a chasm, even though they know there really is no chasm. See supra note 30 and accompanying text.

74 See, e.g., CAL. PENAL CODE § 243.4(a)(1) (“Any person who touches an intimate part of another person, if the touching is against the will of the person touched, and is for the specific purpose of sexual arousal, sexual gratification, or sexual abuse, is guilty of misdemeanor sexual battery . . . .”).

75 RESTATEMENT (SECOND) OF TORTS § 21.

76 MODEL PENAL CODE § 211.1(2)(a).

groping will be more upsetting to many people than getting an unwanted tweet or an email expressing sexual desire.

And peoples’ reactions may well depend on how developed and personalized their avatar is, something that differs from platform to platform and game to game, and that is likely to change over time. Perhaps virtual groping will be upsetting enough to treat it as the sort of action that criminal law ought to, in principle, forbid, if not now than in the near future. This question likely can’t be resolved until we have more experience with how people actually feel in such situations.

Nonetheless, here too, as in the indecent exposure scenario, there is reason to be skeptical of whether criminal law can and should apply. First, as always, is the Bangladesh Problem: Few police departments will be eager to extradite someone from another country or even another state simply because he made gestures, however disquieting, in a virtual reality game. Even police officers who greatly respect women’s bodily integrity may be hesitant to use a great deal of resources to deal with people who, after all, did not literally touch anyone.

Second, here too technologically enabled self-protection may be available. The physical structure of the real world is notoriously tolerant of people coming very close to you. Protection from unwanted touch has to rely on legal rules, social mores, and the threat of violent self-protection.

But the code-as-law of the VR world can easily forbid avatars from approaching within some perceived distance of you, or forbid particular people from doing it, or forbid this except in certain games. Indeed, VR developers have already offered this as a response to Belamire’s article; as the author of the VR game that Belamire had been playing wrote,

We should have prevented this in the first place. While QuiVr is still in pre-release alpha, we’d already programmed a setting into the game called your, “Personal Bubble,” so other player’s hands disappear if they come close to your face. This way, the rare bad-apple player can’t block someone else’s view and be annoying. The arrows that get shot at you stick in your helmet, which is good for a laugh, but they do no damage and quickly disappear so they don’t get in the way. We hadn’t, though, thought of extending that fading function to the rest of the body....

I called Jonathan, who is . . . the original creator of QuiVr . . . . He’d already seen the article—his girlfriend had sent him the link—and he had spent the morning changing the game to extend the Personal Bubble; now, when the setting was turned on, other players faded out when they reached for you, no matter their target, chest included. . . . It was a possible solution; no one should be able to treat another player like the author had been treated again.78

---

Indeed, the author suggested other technologically enabled self-protection options, including ones that come across as more active self-defense (or, if you prefer, retaliation)—perhaps, for instance, allowing a player to "reach[] out with a finger, and with a little flick, sent [the other] player flying off the screen like an ant."79 One can even design the game so that this feature can only be used against those avatars who come too close to one's own (or else the flicking could itself become a form of unprovoked aggression). Or the VR or AR company can set up a bubble feature that excludes some avatars but not others that the participant has placed on a "close approach permitted" list.

If people behaved better, none of this would be needed. But given that people do behave badly, VR and AR technologies sometimes offer better tools for dealing with bad behavior than the physical world does.

5. Crimes that can’t be easily technologically avoided—extortion, threats, and the like

This cheapest-cost-avoider/you-could-have-avoided-it-yourself argument, of course, only works for crimes that are indeed avoidable with technical measures. Many will not be. For instance, there is no technical feature that you can use to avoid someone trying to extort money from you in VR or AR by threatening you with attack in the real world ("I know where you live in the real world, and I’ll burn down your house if you don’t pay me $10,000 worth of VR goods"). There, you will have to rely on normal law enforcement and normal criminal law, subject to the constraints imposed by the Bangladesh problem.

But it’s no accident that extortion is not usually seen as a street crime, in the sense of a crime that is generally committed through physical presence (as opposed to through potentially long-distance communication, even absent VR). For a considerable amount of the street crime that has a VR analog, technologically enabled self-protection is a possible protection—and failure to use such self-protection may lead to the police having little sympathy for your plight.

6. AR crimes that can’t be easily technologically avoided—startling

Finally, let’s note one crime that is especially likely to be dangerous in AR: deliberately or recklessly startling someone in a way that’s likely to dangerously interfere with his physical-world tasks.

Say I know that you’re driving with your AR set engaged, and I deliberately appear in your field of vision—not just as me, but as a giant, loud, fire-breathing dragon (or perhaps as a very attractive naked person of whatever sex you find attractive). Or perhaps I happen to know that you have a fear of spiders, so that’s the avatar I choose, in an attempt to startle you. You are indeed startled and get into an accident.

79 *Id.*
(In principle, this might happen even in VR, but the risks are greater when people are using AR, which they might do even when driving or walking down a busy street.)

That might well be a crime, such as reckless endangerment,80 or negligent homicide or involuntary manslaughter if someone dies.81 It could certainly be a tort (more on that in Part III). This would be one of the few scenarios—strobe lighting being the other—which could actually cause physical injury. And it is also not easily avoided through technological self-help measures.

But as a practical matter, this is likely to be a special case of the broader problem: AR can be distracting, especially for drivers82 but also for people walking near traffic and other hazards. AR designers will have to find some way of dealing with such normal incidental distractions; that might likewise be useful for dealing with deliberate but much more unusual distractions.

B. Diversity of Sensescape

Technological self-protection options, if properly designed, can do more than just make it unnecessary for police to intervene—such options can make possible a broader diversity of VR environments from which users can choose. Indeed, they can make it possible to have a broader diversity of experience within the same environment.

Consider the indecent exposure hypothetical. Some people may like being in an environment where some of the avatars they see are naked, or where they themselves come across as naked. They might be consciously seeking titillation. But they may also want realism, for instance if they are engaged in VR tourism to a place (or time) where women go topless.

Or they may want fantasy, if they want to visit a fictional world where nudity taboos are absent (or are different), or where mythical but part-human creatures (think satyrs or centaurs) are normally nude. Or they may be nudists, who feel more comfortable coming across as naked, and being around other people who do the same.

Leaving the policing of nudity taboos to each VR environment—or perhaps to each user in a VR environment—can increase people’s options. Some people will go to the nudist environments; others will go to nonnudist ones.

---

80 Model Penal Code § 211.1(2)(a).
81 Model Penal Code § 210.4.
But beyond that, if the technologically enabled self-protection measures are available, different users will be able to have different experiences in the same VR environment. Those who like casual nudity can see nudists’ avatars as nude. Those who dislike it can see the same avatars as clothed. So even if you need to be in a particular VR environment (for instance, because your job so requires), you can experience that environment without the nudity.

To be sure, some people may have moral objections even to voluntary nudity; consider the public nudity laws that ban nudity even in strip clubs. But we think these objections should not be particularly strong. Even if bans on consensual public nudity are constitutionally permissible, we doubt that they are good policy; it’s better, we think, to live and let live on such matters, leaving people free to choose from a diverse range of environments. That is even more true when the environment itself is one you can choose whether or not to participate in.

The de facto toleration of nearly all online pornography throughout the U.S., even of pornography that is likely theoretically punishable as obscenity, supports our view. At least on the Internet, the Sexual Revolution is over, and sex won: Where the sex is entirely online, without bricks-and-mortar stores that are seen as potentially attracting bad elements, it is generally tolerated. And if the toleration stems from difficulty of enforcement as much as from thoroughgoing acceptance, that would apply at least as much in VR as well.

The strobe example likewise shows the value of technologically enabled self-help. Some people like strobe lighting, for aesthetic reasons. It’s also a good way of getting people’s attention for things like alarms, especially for the hard of hearing. And epilepsy can be triggered by other near-strobe effects that are likewise valuable for aesthetics or for verisimilitude. Giving people an option to decide whether to block strobe effects will maximize the number of possible virtual environment designs, while maximizing the virtual environments’ accessibility to the small minority that suffers from epilepsy as well as the majority that doesn’t.

84 See, e.g., State v. Louisiana Toy Co., 483 So. 2d 1264, 1268 (La. Ct. App.) (“[T]hat prosecutions for obscenity might be rare or even erratic does not mean they are arbitrary or discriminatory.”)
86 Photosensitivity and Seizures, Epilepsy Foundation, http://www.epilepsy.com/learn/triggers-seizures/photosensitivity-and-seizures ("Natural light, such as sunlight, especially when shimmering off water, flickering through trees or through the slats of Venetian blinds," “Television screens or computer monitors due to the flicker or rolling images,” and “Certain visual patterns, especially stripes of contrasting colors.”).
Finally, though more controversially, diversity of options may be relevant even for virtual groping. Most people, we believe, wouldn’t like being virtually groped by people they just met online. But people’s preferences when it comes to sexual (and sexualish) matters are notoriously diverse, and often unexpected to those who don’t share the preferences. And that is especially so when the sexual behavior is relatively low-risk: not sex in the absence of clearly communicated consent; not even physical groping in the absence of clearly communicated consent; but the visual perception of gestures that appear similar to what physical groping would look like in the real world.

Some people, for instance, might find such attempts to be more akin to flirting than to assault, and find the possibility of such attempts to be welcome, even if they rebuff individual instances of the attempts. Indeed, there might be VR spaces where people go in order to meet prospective sexual partners (whether for in-person sex or for the VR equivalent of phone sex) in which such behavior is part of the courtship ritual.

Likewise, there might be VR games in which this behavior is allowed. This could be for verisimilitude: If you’re playing a game set at the Bristol docks in 1750, you might want rude behavior, and the reactions to the behavior, to be part of the gameplay. Or it could be for titillation: We can imagine that some people might fantasize about rough or nonconsensual sex and enjoy the fantasy even though they wouldn’t enjoy the physical experience; a VR version may provide those people with the right combination of realism and fantasy.

Of course, most people, like Belamire, won’t want to be groped. But that’s the point: There is a diversity of sexual preferences. VR offers the possibility that people can control their environment and consent to only what they want.

C. Defaults and the initial intrusion

All this, of course, raises a question that’s a version of Justice Stevens’s Paciﬁca argument. All the self-protection tools involve the likelihood that people will often be exposed to misconduct—such as loudness, public nudity, or virtual groping—one, or perhaps once per offender, before they block the misconduct. To be sure, potential victims might be able to prevent some of the misconduct at the outset, with the proper configuration, but practically they will often not think about it until the first incident. The tools that will likely be available thus allow what one might see as an initial intrusion, but can stop recurrences.

Should that be considered acceptable? Or should the criminal law try hard to prevent even the initial intrusion? Recall Justice Stevens’ specific analogies:

To say that one may avoid further offense by turning off the radio when he hears indecent language is like saying that the remedy for an assault is to run away after the first blow. One may hang up on an indecent phone call, but that option does not give the caller a constitutional immunity or avoid a harm that has already taken place. 88

And indeed the law generally forbids unwanted physical “blow[s]” (though not all unwanted touching), and all indecent telephone calls, including the initial call. 89 On the other hand, the law doesn’t forbid unwanted indecent mailings—rather, it lets residents demand that the mailer stop sending them offensive material. 90 Likewise, the law can’t categorically forbid door-to-door leafleters from coming to your home, though it can forbid them once you’ve put up a “No Soliciting” sign. 91 And many, us among them, don’t think Pacifica is a shining beacon of First Amendment jurisprudence. 92

Even in circumstances where people can practice self-help once a threat is identified, then, the law can and should set defaults. A virtual environment could be configured to permit strobing except for those who opt out, or to forbid strobing except for those who opt in. Likewise for showing nude avatars, or allowing physical approaches within some distance.

The law could thus take the view that even an initial intrusion of this sort is a crime unless (1) the environment forbids the intrusion by

---

88 FCC v. Pacifica Found., 438 U.S. 726, 749 (1978) (Stevens, J., lead op.).
91 Martin v. City of Struthers, 319 U.S. 141 (1943).
92 FCC v. Fox Television Stations, Inc. (II), 132 S. Ct. 2307, 2321 (2012) (Ginsburg, J., dissenting); FCC v. Fox Television Stations, Inc (I), 556 U.S. 502, 532–35 (2009) (Thomas, J., dissenting). Indeed, Justice Stevens himself erred in trying to explain how Pacifica was consistent with Justice Stevens’ more recent opinion in Reno v. ACLU, 521 U.S. 844 (1997). “Unlike the regulation[] upheld in Pacifica,” Justice Stevens wrote, “the scope of the [Communications Decency Act] is not limited to commercial speech or commercial entities.” Id. at 877. But the Pacifica regulation was not limited either to commercial speech or to commercial entities; the broadcast in Pacifica itself was noncommercial speech carried by a nonprofit, noncommercial radio station. Application of Pacifica Found., 50 F.C.C.2d 1025 (1975) (describing Pacifica as “the licensee of noncommercial educational FM Stations” including “WBAI, New York”); In re Citizen’s Complaint Against Pacifica Foundation Station WBAI (FM), 56 F.C.C.2d 94 (1975), eventually aff’d sub nom. FCC v. Pacifica Found., 438 U.S. 726 (1978) (confirming that the broadcast was indeed on WBAI). This helps show, we think, how hard Pacifica is to reconcile with modern First Amendment law.
default and (2) the user has expressly allowed the intrusion. This might mean that:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the environment lets you supply both a clothed avatar and a nude avatar, and by default has others only see your clothed avatar,</td>
<td>then there’s no indecent exposure even when you create a nude avatar, since only people who have affirmatively chosen the see-nudity option will see the nude avatar.</td>
</tr>
<tr>
<td>If the environment lets you supply both a clothed avatar and a nude avatar, but by default lets people see the nude avatar,</td>
<td>then you’re guilty of indecent exposure for using a nude avatar, since people are entitled to be shielded from even the initial intrusion of nudity into their visual field.</td>
</tr>
<tr>
<td>If the environment only lets you supply one avatar, but allows a “clothe this avatar” feature on an avatar-by-avatar basis,</td>
<td>then you’re likewise guilty of indecent exposure for using a nude avatar.</td>
</tr>
</tbody>
</table>

Alternatively, the law could take the view that certain initial intrusions aren’t a big enough deal to justify criminal punishment, so long as they can be quickly dealt with by the offended user. Or the law could take the view—which would yield the same result, though on a different rationale—that the decision to enter the VR environment is consent enough to such quickly-dealt-with initial intrusions, even when entering the VR environment may be required by your desire to access important resources (your VR job, your VR educational program, your access to VR shops).

We’re inclined to think that, so long as the initial intrusion is relatively minor, and can be quickly stopped through technological self-help matters, there’s no need to bring the machinery of the criminal law into the matter. (Tort law might be a different story.)

But this judgment will often turn on just what intrusions you think are minor enough: Unwanted noise? Nudity? Strobe lights? Virtual groping? We have views on the relative severity of these—the law should probably prohibit virtual groping without explicit prior consent, but not unwanted noise and probably not nudity—but reasonable people can differ about where to draw the line. And these questions will become especially complicated once we get to VR environments that go beyond the merely audiovisual, a matter we will turn to below.

**D. Beyond the audiovisual: haptic assault**

So far, we’ve talked about harms that can be caused by the audiovisual features of VR—the only features that are well-developed now. But let’s now turn to features that VR is likely to acquire soon: haptics.
Haptics are to touch what are optics are to sight. Existing 2D games have very simple haptics: a Playstation DualShock controller that vibrates when you drive over bumps or run into something, for instance. But the immersive nature of VR can offer quite a bit more.

Gloves that reproduce sensation on fingers are haptics. So are temperature controls that can make VR tourism more realistic. So are devices that could cause feelings of physical resistance, so that a virtual swordfight would yield realistic sensations when your virtual sword hits your virtual opponent’s. And one can also embed haptics and remote control into sex aids—a business called teledildonics.93

Teledildonics raises the possibility of haptic sex crimes. Unconsented-to sexual touching is a serious offense, and should be so even if the person doing the touching is not in the room with you. True, sexually transmitted diseases and unwanted pregnancy aren’t a threat in the virtual world; and some people may be less troubled by unwanted remote fondling through their haptic interfaces than by unwanted in-person fondling. But we think it likely that people will be justifiably upset enough by such unwanted touching that it would merit punishment.

Similar issues come up outside of sex. Say some people enjoy a particular game that’s supposed to simulate a dangerous physical activity (battle, mountain climbing, flying an airplane), but are frustrated that death or injury in the game has no real consequences. They think it makes themselves and other players reckless, and distorts the game’s realism. Playing poker for matchsticks, it is often said, isn’t the same as real poker. Likewise, playing at sword fighting when being speared through the neck just means “Game Over” isn’t as realistic, they think, as it should be.

So they think that players ought to have skin in the game, as it were: Certain events should trigger something bad—not death (they’re not that hard-core) but physical pain. Indeed, paintball players sometimes take the view that the painful sting of being hit enhances the game, by making players work harder to avoid being hit, or just by making the game exciting.94 Likewise, some social psychology experiments punish people who lose a game by requiring them to consume a substance that is extremely unpleasantly bitter, so as to encourage participants to take the game seriously.95

93 No, we aren’t providing a citation. Search for it yourself if you really want to.

94 See, e.g., How to Treat Paintball Welts, https://acpaintball.com/2015/04/22/how-to-treat-paintball-welts/ (“Most players consider paintball well worth the risk of pain, some even welcome the risk to increase the adrenaline and excitement.”).

Imagine then that a VR setup can have an optional hardware feature: a device that produces an electric shock that is not dangerous but is painful. (One might think of it as “algics” rather than normal haptics.) People who want to play Extreme Sword Fights (let’s call it) must have the device attached, and when they are hit with the virtual sword, they get a real shock. Here, unlike our previous examples, we do have actual physical contact with the victim’s body, albeit contact triggered at a distance rather than by someone standing next to you.

So long as the shock really doesn’t pose any serious physical danger, causing the shock by hitting someone in-game wouldn’t be battery. Battery generally requires nonconsensual touching, at least so long as it doesn’t involve a public fight that risks spreading, or serious physical damage that goes beyond mere pain. This is why a wide variety of often painful activities, from football games to mild sadomasochism, are legal. And you consented to be hit by a virtual sword—or at least to run the risk of being hit. By contrast, triggering the haptics outside the game—for instance by hacking someone’s VR rig to give them a surprise electric shock—presumably would be nonconsensual.

So far, so good. But consent in a virtual world has some nuances that we might not expect, as we see in the next section.

E. Consent

Say that you’re playing a game, whether VR or not. One of your fellow players steals some of your in-game currency, or embezzles it or defrauds you of it. That theft can have real-world financial consequences: In-game currency can often be bought and sold for real money, and you can even imagine a system in which your in-game assets are replenished, when needed, directly from your bank account or credit card. In-

---

96 *algia* is the Greek root meaning pain, as seen in words such as “analgesic.”


98 See, e.g., MODEL PENAL CODE § 2.11(2) (providing that consensual conduct is not criminal, even if “it causes or threatens bodily injury,” if “the bodily injury consented to or threatened by the conduct consented to is not serious,” or “the conduct and the injury are reasonably foreseeable hazards of joint participation in a lawful athletic contest or competitive sport or other concerted activity not forbidden by law.”). *But see Commonwealth v. Carey*, 974 N.E.2d 625 (Mass. 2012) (concluding that sadomasochism that risks causing more serious injury remains punishable assault, even when consensual); *Govan v. State*, 913 N.E.2d 237, 242–43 (Ind. Ct. App. 2009) (likewise).
deed, many games have currency top-up systems that let players put
real money in and convert it to virtual money when they run out.99

One way to steal virtual money (or a magic sword, or anything else
of value) would be to hack into your computer, or physically threaten
you in the real world. That sort of behavior should be criminal, though
of course it isn’t easy to get police attention for violations of computer
crime laws—or even for thefts conducted through such violations—at
least unless the crimes cause substantial financial loss.

But our hypothetical player didn’t hack into anyone’s computer, or
do anything else that was outside the understood possibilities of the
game (whether or not it was against the laws announced within the
game). Rather, he just cut off your (virtual) purse and ran off with it. Or
he threatened to have his character kill your character if you didn’t give
him the money. Or you opened your virtual safe to let him take 10 gold
pieces, and he used the access to take 1000.

Games sometimes permit such actions. If I fight your character and
win, I may be able to loot his body. That sort of looting, if it is “theft” at
all, is theft contemplated by the rules of the game. By playing the game
I accepted the risk that I might lose virtual currency to an enemy, just
as I consented in the sword fighting algics scenario100 to the possibility
that I would be hit by a virtual sword.

But now let us assume that what my thief did violates the rules of
the game itself. Should that be a crime from the perspective of American
law? Or should it be just one of the things that happens in the wolf-eat-
wolf world that is Game of Thrones—The Game?101 Indeed, might it be a
valued gameplay feature, which helps create verisimilitude, extra stra-
tegic options, and emotional tension? What kind of goody-goody non-
sense would Game of Thrones—The Game be if all players actually had
to follow Westeros law?

Maybe the remedy for such theft within the game would be an at-
tempt to launch an in-game criminal prosecution, under whatever rules
the game environment allows. (Perhaps trial by combat?) Or maybe
such thefts would be deterred by the threat of blood feud, or of magical
or divine retaliation, all within the game. Just as the possibility of bro-
ten treaties is a valuable feature of games such as Risk and Diplomacy,
the possibility of theft may be a valuable feature of other games.

One way of conceptualizing this is that playing a computer game
(VM or otherwise) might by default consent to everything that could
physically happen within the game, whether or not it is legally allowed

99 Hayley Tsukayama, Diablo 3 Auction House to Charge Real Money for In-
100 See supra Part II.D.
101 We’re not sure how much outright theft is currently physically possible
in Game of Thrones—The Game; but if it isn’t, it should be.
within the game. This has been labeled the “magic circle” excluding real law from virtual worlds.102

A game could announce that it is departing from the default. For instance, gamers are often frustrated if their opponents use bots or cheat codes to circumvent the limitations under which everyone else operates.103 If game makers ban the exploits,104 a player could presumably have a civil or even criminal cause of action against the cheater, just as she could pursue a computer hacker who took valuable data off her laptop. And many games in fact do ban hackers and bots, presumably because they think their players want a level playing field in some respects.

But a rule that violations of in-game laws must be dealt with, if at all, using in-game justice (formal or otherwise) seems to us a sensible default for many games. At least it should be an option, and if it is given as an explicit option, it will be one that many games are likely to choose.105

Yet VR involves more than just games. Some environments, including some VR environments, are likely to be used for straight-up commerce, where people shouldn’t have to expect cheating. “Sure, my store is an elaborate fraud—we goblins are notorious tricksters, and widely known within Middle Earth to be evil” may be an acceptable explanation for a “let the player beware” response in a game, but shouldn’t apply when the store is part of a normal VR shopping mall.106

Again, though, the distinction turns, we think, on consent: One consents to more trickery when one is playing a game than when one is engaging in normal commerce. Presumably in most cases it will be clear which environment is one and which is the other. But perhaps there might be need for clear statement rules, so that fraud and theft of in-VR resources would be noncriminal only if something is clearly labeled as a “game,” perhaps with a requirement that the users specifically acknow-

104 Id.
106 See Greg Lastowka & Dan Hunter, The Laws of the Virtual Worlds, 92 Calif. L. Rev. 1 (2003) (both arguing that virtual property shouldn’t be outside the scope of real-world laws); Fairfield, Magic Circle, supra note 102 (same).
ledge the possibility of fraud and theft as a condition of playing the
game.107

The existence of haptics and algics might also change the calculus.
Return to our example of virtual swordfighting, but now assume that
someone deliberately violates the rules of the game to inflict more pain
than the rules allow.

Say, for instance, that one of the rules of Extreme Swordfighting is
that you don’t hit someone who is already labeled as dead or disabled, or
someone who has surrendered. But say that you keep hitting me after
I’m down, inflicting five shocks in succession rather than the officially
allowed one. I’m very upset by your deliberately sadistic behavior, and I
try to have you prosecuted.108

As with the theft in the previous subsection, one possible reaction is
that this is a crime: I have consented only to those shocks that are with-
in the rules of the game. You have violated the rules, and thus exceeded
the consent.

But another possible reaction is that I’ve consented to a broader
range of behavior: By playing the game with my shocker enabled, I have
consented to anything that you can do (at least short of serious physical
injury) with that shocker; indeed, the possibility of cheating may be an
understood part of the game.

Here too self-help may play a role. It seems very likely that algenic de-
vices, such as the electric shockers, will come with an easy override, and
may even be programmable to (for instance) limit the shocks to no more
than one every ten seconds, so one will have the time to engage the
override. Certainly manufacturers would have lots of incentive to pro-
vide such features and tout them to users.

And if you play a game in which repeated shocks are possible, and
don’t engage any override that blocks such shocks, that itself might be
seen as consent to the shocks—even when the shocks violate the in-
ternal game rules. If you don’t like it, shift to a different setting. This will
make it possible for you to enjoy more self-protective gameplay, while
others can enjoy more transgressive gameplay.

In principle, sexual haptics have some similarities to algics and to
other haptics. One doesn’t have to place haptics on one’s erogenous
zones, or to enable them even if one has them—just as one doesn’t have
to have algics, or to turn on the algics. (Again, VR and AR are better
that way than real reality is: Our bodies have biological haptic and algec

pers.cfm?abstract_id=1702427 (working paper 2014) (noting the risk of theft in
virtual environments and the ways in-game rules might deal with it).

interfaces that are accessible to passersby, whether or not we want to turn them on.)

At the same time, if one walks into a party with one’s haptics turned on, one might be expecting—as in the real world—that one’s lover would feel authorized to, say, covertly rub one’s thigh, but that a stranger would not. And because unauthorized sexual touching is seen as much more intrusive and offensive than even unauthorized pain in a sword-fighting game, there may be good reason to require some overt opt-in before such touching, at least when it moves beyond the thigh and on to the breasts or genitals (though again recall that this becomes a problem only if one attaches haptics to those parts of one’s body).

These questions, of course, are already famously contested and complex in the real world. We expect them to be similarly disputed in VR and AR as well, especially when one moves away from the pretty clear taboos (you don’t touch someone’s genitals unless there are strong indications of consent) to borderline questions (when is it OK to kiss someone? to caress someone’s butt when dancing?). At this point, without more knowledge about how sexual haptics are likely to be used, we’re not sure what the right answer will be, but we think the problem is bound up with how we think about consent in a particular virtual environment.

F. Consent and impersonation

Consent in the physical world—to sex, to hitting, or to fraud—presents a variety of legal issues. But VR and AR add a couple of new twists. The first, which we raised above, is that consent can always change with the environment (game-playing vs. shopping, for instance), and people may switch virtual environments more often than physical environments.

A second way VR complicates the picture, though, is that identity is malleable. If I convince someone to have (virtual) sex with me by pretending to be her boyfriend, that too seems like something at least tort law would be inclined to punish, though it almost certainly isn’t rape under the current U.S. definition of the term.109 Perhaps intentional infliction of emotional distress?110 Perhaps the tort of battery, on the theory that the consent defense is made unavailable because of the fraud?111


110 See, e.g., RESTATEMENT (SECOND) OF TORTS § 46.

111 See, e.g., RESTATEMENT (SECOND) OF TORTS §§ 18, 19 (nonconsensual offensive touching can be battery); id. § 892B(2) (consent procured by fraud may be invalid).
Here, too, the possibility of technological self-help might incline the law not to be too quick to intervene. In a world in which people can change their appearance at will, experienced VR users will learn not to assume that we are who we say we are, merely based on our avatars’ names (TaylorSwift? JaneSmith?) and appearance. So before handing over money (or engaging in sex) you will probably want to verify that your prospective partner is who he or she appears to be, perhaps with a shared password or some sort of persistent actual identity.

But not all VR environments will want to require people to disclose their real identities, just as some but not all web pages have “real name” policies. So the law may want to police cases of intentional misrepresentation, at least when there are significant consequences at stake. And, subject to the Bangladesh problem, identity fraud that yields sufficiently serious losses may be one of the acts in which the default legal rule doesn’t give the perpetrator one free pass.

III. TORT, INTELLECTUAL PROPERTY, AND VR/AR PROVIDER LIABILITY

A. Direct tort lawsuits against offenders: the causes of action

So far, we’ve been talking about the criminal law; what about tort law? Let us turn first to the direct tort liability of some of the potential offenders we described above.

In theory, such liability might be possible in many of the circumstances we have identified, even if criminal law won’t apply. For instance, using strobe lights to deliberately cause a seizure in a person one knows is epileptic is likely at least negligence, and possibly also a form of battery, though that question is complicated.112

For the other scenarios, tort liability would be more of a stretch, but not implausible. Disturbing the peace might be recharacterized as nuisance, at least in a suit brought by “nearby” VR or AR stores whose business is interfered with by the screaming; but, especially as to VR, that would require nuisance law to be modified, for instance by treating VR “places” as tantamount to “uses of land” which nuisance law protects.113 Nuisance also generally requires either long-term interference or especially serious interference;114 disturbing the peace law punishes even brief incidents.

Virtual groping might be treated as intrusion upon seclusion; though it happens in “public” places, the intrusion tort can apply even there, to behavior that is seen as intruding on one’s bubble of personal

112 RESTATEMENT (THIRD) OF TORTS: INTEN. TORTS TO PERSONS § 101.
113 RESTATEMENT (SECOND) OF TORTS § 822.
114 RESTATEMENT (SECOND) OF TORTS §§ 821D, 821F cmt. g.
space.\textsuperscript{115} Indecent exposure might qualify as well. Both might also constitute intentional infliction of emotional distress, even in the absence of physical touching, on the theory that they are both “outrageous,”\textsuperscript{116} though that tort generally requires a showing of severe emotional distress where there is no physical contact.

Tort law can also reach a wide array of conduct that wouldn’t be a crime even in the physical world. Defaming a VR avatar should be a tort, even if the avatar is pseudonymous.

One of us has had an extended debate with a well-respected federal judge who believed it was impossible to defame an avatar because avatars weren’t real, so their reputation couldn’t be injured.\textsuperscript{117} This “it’s just a game” sense might pervade VR for some time in the courts, in part because most judges are unlikely to be early adopters of VR. But we think such a view is misguided.\textsuperscript{118}

Corporations can sue for defamation, because people invest time and money to create reputational capital for the corporation.\textsuperscript{119} There’s no reason why the same wouldn’t apply to a pseudonym that is used to do business, in VR or otherwise—or to one that is used for ordinary life. The idea that falsehoods that damaged the reputation of Mark Twain weren’t defamatory unless they expressly mentioned Samuel Clemens strikes us as unsound.

The damages to a pseudonym’s reputation might be less in many situations than the damages to a real person’s reputation, because many pseudonyms have built up less reputational capital, and people can take on new ones with little loss. But they could be quite great in other situations, if—as is true in some Internet circles and will likely be increasingly true in VR—the pseudonym or avatar is better known than the person’s name, which might be obscure or even deliberately concealed.

\\textsuperscript{115} Restatement (Second) of Torts § 652B.

\textsuperscript{116} See, e.g., State Rubbish Collectors Ass’n v. Siliznoff, 240 P.2d 282 (Cal. 1952) (threats); Bundren v. Superior Court, 145 Cal. App. 3d 784 (1983) (telephone calls rudely demanding payment from a person who the caller knew was recovering from surgery); Esposito-Hilder v. SFX Broadcasting, Inc., 665 N.Y.S.2d 697 (N.Y. App. Div. 1997) (radio talk show describing plaintiff as the “ugliest bride” in a newspaper’s wedding announcement section). Reasonable minds could differ over whether virtual groping should be thought to involve “physical” touching, but the conduct might reasonably be viewed as outrageous enough that it shouldn’t matter.

\textsuperscript{117} Lemley, Dubious Autonomy, supra note 102, at 576. No, we won’t tell you who it was. What happens in the hallways outside conferences stays in the hallways outside conferences.

\textsuperscript{118} Id; Lastowka & Hunter, Laws, supra note 106, at 72–73.

Most readers probably couldn’t come up with the real name of The Weeknd, but that doesn’t mean we couldn’t defame him.120

B. Direct tort lawsuits against offenders: practicalities (and impracticalities)

Tort lawsuits against VR and AR offenders have one important advantage over criminal prosecutions: They are available even when the police are unwilling to intervene. For example, even if the police don’t want to spend their time on a difficult investigation—especially when they think the complainant could have avoided the problem using technologically enabled self-help—the complainant can still demand his day in court.121

Practically speaking, though, we doubt that people will often sue each other for most VR or AR behavior. First, again, there is the Bangladesh problem. VR torts might involve tricky jurisdictional questions; if you’re screaming in a VR forum from your apartment in Poland, is it fair to require you to answer lawsuits filed in San Francisco or in Buenos Aires?

People have litigated that question extensively in Internet cases.122 But even if a court in, say, California concludes that it has jurisdiction over the Pole (perhaps because the Pole targeted strobe lights at a person who he knew to be in San Francisco), enforcing a judgment against someone half a world away would likely be very hard, and in any event many defendants would lack the money to satisfy a judgment.

Second, while police refusal to go forward wouldn’t be a barrier to civil lawsuits, the cost of such lawsuits might be. However distressed one might be by virtual groping, it’s unlikely that one would be willing to spend tens of thousands of dollars tracking down the culprit, suing him, and trying to recover the judgment. Some people might, perhaps to send a message, but that would be rare.

And abbreviated procedures that are aimed at making lawsuits cheaper and easier—such as small claims trials or restraining orders—won’t help much. A small claims court might be reluctant to allow a lawsuit against someone far away, even if jurisdiction is in principle available;123 any judgment, moreover, would still be costly to enforce.

120 Try this: Selena Gomez is too good a singer for him.
121 Comparative negligence is generally not a defense to intentional torts, though of course outright consent would be. RESTATEMENT (SECOND) OF TORTS § 892A.
123 Some small claims courts are limited in their jurisdiction over out-of-state defendants. See, e.g., N.Y. CITY CIV. CT. ACT § 1801 (limiting New York
And the police may be as reluctant to go after a faraway restraining order violator as they are to go after a faraway flasher or screamer.

C. Tort lawsuits for physical injuries to outsiders

VR and AR users will sometimes also physically injure outsiders. A player chasing a Pokemon might run into someone, or might cause damage by trespassing on someone’s property. A VR user wearing a headset might walk into a houseguest. Those injuries will often be the fault of the user herself, or someone else using the system. But sometimes the injury may result from flaws in the design of the VR or AR hardware or software itself. And that opens a second, more practical possibility: suing the hardware or software designer itself.

These design defects should be analyzed using normal tort law rules. Just as a car or bicycle manufacturer may be liable for physical injuries caused by defects in the device, so a VR or AR equipment manufacturer may be liable. If a defect in an AR headset, for instance, causes it to flash a very bright light that temporarily blinds users and leads them to run into people, that sounds no different from a defect in a bicycle’s brakes that leads the rider to run into someone.

Many such defects would stem from the VR or AR system providing incorrect information to people—for instance, an AR system defectively instructing you to turn in the wrong place, or a VR system that claims to sense whether someone walks into your room but then defectively fails to properly report it. The fact that information is involved complicates things, because the publication of information—even false information—might implicate the First Amendment. For instance, the Ninth Circuit has held that the publisher of the Mushroom Encyclopedia isn’t strictly liable when you poison yourself because the Encyclopedia had bad information. On the other hand, the publisher of a flawed aeronautical chart is strictly liable when you use the chart to fly into a mountain.

City small claims courts to actions where “the defendant either resides, or has an office for the transaction of business or a regular employment”).


125 Richard Winton, *Police fear the dark side of ‘Pokemon Go’*, L.A. TIMES, Jul. 12, 2016. We set aside VR or AR defects that cause pure trespass, without damage. Negligent trespass is generally not actionable absent damage. RESTATEMENT (SECOND) OF TORTS § 165. Likewise, a manufacturer’s negligence in leading someone to trespass should generally not be actionable without damage, either.

126 Winter v. G.P. Putnam’s Sons, 938 F.2d 1033 (9th Cir. 1991).

127 Brocklesby v. United States, 767 F.2d 1288 (9th Cir. 1985).
Even if the Mushroom Encyclopedia case is correct, we think incorrect directional information provided by VR and AR that makes you walk into a wall is more like the incorrect directional information provided in aeronautical charts. Even more than with charts, people generally rely on instructions provided by their VR and AR headsets automatically, with no opportunity for reflection. Indeed, that is the whole point: If a VR headset shows a pathway for you to walk down, you’re supposed to walk down it. That assumes that the VR system is supposed to know where walls and other obstacles are, but they generally do.\textsuperscript{128}

The Ninth Circuit’s effort to distinguish aeronautical charts from the Mushroom Encyclopedia is a little opaque, but it supports our position:

Aeronautical charts are highly technical tools. They are graphic depictions of technical, mechanical data. The best analogy to an aeronautical chart is a compass. Both may be used to guide an individual who is engaged in an activity requiring certain knowledge of natural features. Computer software that fails to yield the result for which it was designed may be another. In contrast, The Encyclopedia of Mushrooms is like a book on how to use a compass or an aeronautical chart. The chart itself is like a physical “product” while the “How to Use” book is pure thought and expression.\textsuperscript{129}

Even if a mushroom encyclopedia is “pure thought and expression,” because it teaches how to do something, a VR or AR headset is far from that. Instead, it’s an even more automatic “guide” than a compass: It offers visual cues that the users are meant to follow without thinking. It is like a physical product, albeit one composed in large part of information.

\textbf{D. Using tort law to draft VR/AR operators into preventing misbehavior by users}

Plaintiffs won’t want to limit suits against operators just to errors in the systems themselves; they may also want to hold operators liable for users’ misconduct. Individual users may be hard to sue, but VR and AR operators—both software and hardware providers—will not be. They will usually be easily identifiable, and will often have assets in many of the jurisdictions in which their users live. Users who believe they have been harmed while participating in a VR environment might thus sue, not the tortfeasors themselves, but the VR operators for negligently contributing to their injuries.

Generally speaking, American negligence law holds that people who provide physical spaces—such as shopping malls—have a duty of rea-

\textsuperscript{128} See, e.g., Oculus, \textit{Oculus Guardian System}, https://developer3.oculus.com/documentation/pcsdk/latest/concepts/dg-guardian-system/ (“The Oculus Guardian System is designed to display in-application wall and floor markers when users get near boundaries they defined.”).

\textsuperscript{129} Winter v. G.P. Putnam’s Sons, 938 F.2d 1033, 1036 (9th Cir. 1991).
sonable care to safeguard their business visitors from physical harm.\textsuperscript{130} That includes harm from criminal attack.\textsuperscript{131} The theory is one of negligence, not of strict liability or vicarious liability: A shopping mall owner wouldn’t be liable simply because a visitor was criminally attacked by another visitor.\textsuperscript{132} But if there were reasonable, cost-effective, not unduly burdensome steps that the owner could have taken to prevent reasonably foreseeable crime, and the owner didn’t take the steps, then the owner could be held liable.\textsuperscript{133}

This negligence theory would clearly apply to AR that is under a physical property owner’s control. Say that a shopping mall provides an AR network to its customers—perhaps so they can more easily find their way to stores, or see what’s available in a store, or just communicate with friends and thus better enjoy the shopping experience. And say that someone uses the network to target a customer for a strobe-light attack. If (1) the attack was reasonably foreseeable, (2) the AR software could have easily and inexpensively provided an option that customers could use to block strobing, but (3) the AR software failed to do that, then the shopping mall owner might well be liable for any damage that the attack caused. There would be no need for any extension of existing law; that would already be the result today.

But what about VR, which we use on our own real estate? Or what about an AR system that is provided entirely by AR operators who are unrelated to any shopping mall that we might happen to be visiting? There, the existing duty of a property owner to business visitors wouldn’t arise. Instead, courts would have to consider whether to recognize a new duty, not based on ownership of real estate but based on ownership of “virtual estate,” in the sense of a VR environment that feels to people like a “place,” even if it is not one, or an AR environment that is superimposed on the places that people are visiting.

The rationale for such a duty might be that the VR or AR operator, like a real estate owner, is uniquely situated to provide software protections that users cannot themselves provide.\textsuperscript{134} Conversely, if the VR and

\begin{footnotes}
\footnote{130}{RESTATEMENT (THIRD) OF TORTS: PHYS. & EMOT. HARM § 51 (2012).}
\footnote{131}{Id.}
\footnote{132}{See, e.g., Castaneda v. Olsher, 162 P.3d 610 (Cal. 2007).}
\footnote{133}{See, e.g., Kline v. 1500 Massachusetts Avenue Corp., 439 F.2d 477 (D.C. Cir. 1970). If the attack was unforeseeable, then the attacker’s voluntary act would be viewed as “breaking the chain of causation,” and the shopping mall’s actions would be seen as not being a proximate cause of the attack. But if the attack was foreseeable, proximate cause would be seen as present even though the immediate cause of the harm was the attack itself. See, e.g., RESTATEMENT (THIRD) OF TORTS §§ 19, 34.}
\end{footnotes}
AR environments are open enough that people can easily buy and run their own apps that provide, say, anti-strobing protection, that would cut against imposing such a duty on the VR/AR operators.

Perhaps, though, such a new duty wouldn’t even be necessary, because—unlike in the physical world—VR and AR operators are, however unintentionally, affirmatively contributing to VR- and AR-based attacks, rather than just failing to stop them. If I can send you stroboscopic images via a VR system, the VR system is itself an unwitting participant in the process, a factual cause of any injury you suffer.

This doesn’t make it strictly liable, of course. But perhaps it does impose on it a duty of reasonable care to make sure that its system doesn’t cause such harm. As the Restatement (Third) of Torts puts it, “An actor ordinarily has a duty to exercise reasonable care” when “the actor’s . . . course of conduct results in greater risk to another than the other would have faced absent the conduct,” including “by exposing another to the improper conduct of third parties.”\(^\text{135}\) This duty is the foundation for many negligence theories, such as negligent entrustment and negligent supervision:

- If (1) I give you access to a car or a gun, (2) I should have known that you couldn’t be trusted with such devices, and (3) you do harm someone by misusing the device, then I can be sued for negligent entrustment (on the theory that I’ve affirmatively contributed to the harm by lending you the device).

- If (1) you are an independent contractor whom I’ve engaged, (2) I fail to reasonably supervise you to make sure that you aren’t misusing your powers under the contract, and (3) you do cause harm through such misuse, then I can be sued for negligent supervision (on the theory that I’ve affirmatively contributed to the harm by bringing you into my project).\(^\text{136}\)

Likewise, if we cross negligent entrustment and negligent supervision, we get the following duty, which is already long established in copyright infringement as well as some tort cases:

- If (1) I give you access to my flea market, (2) I fail to reasonably supervise you to make sure that you aren’t selling copyright-infringing products, and (3) you do sell such products, then I can be sued for contributory copyright infringement.\(^\text{137}\)

\(^\text{135}\) Restatement (Third) of Torts: Phys. & Emot. Harm § 7(a) & cmt. o.


\(^\text{137}\) Fonovisa v. Cherry Auction, 76 F.3d 259 (9th Cir. 1996). This duty is limited by statute for online service providers, though not entirely eliminated. 17 U.S.C. § 512.
• If (1) I give you access to my computer system, (2) I fail to reasonably supervise your use of the system, and (3) you use it to distribute nude photos of your stepdaughter, then I could be held liable for negligent supervision. By the same logic,

• If (1) I give you access to my VR environment, (2) I fail to reasonably supervise your use of the environment, and (3) you use it to tortiously injure someone, then I could be held liable for negligent supervision.

We think courts should hesitate to impose such liability, especially when the proposed supervision or precautions would seriously interfere with other users’ privacy or freedom. Say, for instance, that Tom defrauds Paul while using the Delta Corporation’s VR environment; Tom had a past criminal conviction for fraud; and Delta could have prevented the fraud by just doing a background check on all its users (assume it has their names because it requires them to provide nonanonymous credit cards to participate).

If Paul can successfully sue Delta for negligently enabling this fraud—essentially by negligently entrusting the system to the known fraudster third-party Tom—then Delta would have a strong incentive just to bar people with criminal histories from its system. Or if Paul can successfully sue Delta for negligently enabling the fraud by failing to warn people of Tom’s criminal history, then Delta would have a strong incentive to overtly label everyone with a criminal conviction who is using its system. (Perhaps a scarlet F, for fraud, on the avatar’s chest?)

Such an approach might be appealing to some, despite the burden it imposes on user privacy and the extra burden it places on people with criminal convictions even after they have served their sentences. VR and AR environments might want to tout their background checks as a means of attracting users, just as Uber publicizes that it does background checks on its drivers. And perhaps a legislature might conclude that VR and AR companies should have a duty to do this as well, though this might raise interesting First Amendment problems.

But we don’t think that juries should be making such decisions, especially on an ex post basis, in a case brought when plaintiff has been

138 Doe v. XYC Corp, 887 A.2d 1156 (N.J. Super. Ct. App. Div. 2005). That case involved misuse of a computer system by the employee of the system’s owner; but its logic didn’t turn on the employment relationship, and would apply to other system users as well.


140 Stephanie Rosenbloom, New Online-Date Detectives Can Unmask Mr. or Ms. Wrong, N.Y. TIMES, Dec. 18, 2010.
injured and when the effects of imposing liability will be felt by third parties who aren’t present in court. Courts ought to hold as a matter of law that there is no tort law duty to impose such privacy- and liberty-compromising precautions.\footnote{See Eugene Volokh, \textit{Tort Law vs. Privacy}, 114 COLUM. L. REV. 879 (2014).}

If those precautions are to be legally required, they should be required only as a result of a legislative decision directed to certain specific kinds of precautions and specific kinds of misconduct, not a jury verdict that could arise in any VR negligence case. The law does not similarly require Internet service providers or cell phone providers to supervise the conduct of their users, at least outside the bounds of contributory copyright infringement. And we worry that the consequences of imposing such a duty would cause other, larger problems: restricting user privacy and limiting what individuals can do even with consent.

At most, courts should allow such negligent supervision lawsuits only when the claim is that defendant failed to implement reasonably inexpensive and effective technological self-help measures that don’t involve excluding users or disclosing information about them. Even then we’re not sure that such measures should be required through the unpredictable operation of the tort liability system, as opposed to through clearer, narrow regulations or through market pressure. But at least such requirements would increase the diversity of choices available to users, rather than decreasing them; more on this diversity shortly.

\textbf{E. 47 U.S.C. § 230 as a limit on VR/AR operator liability}

We also think it’s likely that, under current law, VR/AR operators would be immune from liability for most misconduct by their users, because of 47 U.S.C. § 230. Section 230 generally bars any “interactive computer service” provider from being held liable based on “information provided by another information content provider.”\footnote{47 U.S.C. § 230 (2012).} This is why, for instance, services such as Yelp, the Washington Post, YouTube, and America Online aren’t liable for defamation, invasion of privacy, or intentional infliction of emotional distress in items posted by their users.\footnote{Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997), cert. denied, 524 U.S. 937 (1998).}

The story of § 230 is long and oft-told, and we won’t repeat it here.\footnote{See, e.g., Anupam Chander, \textit{How Law Made Silicon Valley}, 63 EMORY L.J. 639 (2014).} But the upshot is that § 230 would probably immunize VR and AR operators from offensive textual, audio, or visual communications by their users, likely including indecent exposure, virtual groping, and the like.
It would probably immunize them even from communications that cause physical harm, such as the deliberately harmful use of strobe lighting.

At the same time, some recent courts have read § 230 more narrowly, perhaps because of a sense that rampant misconduct online requires someone to control it, in an environment where direct lawsuits against those who are misbehaving are impractical, and the police are unlikely to step in.\textsuperscript{145} It is possible, though not certain, that courts will take a similar view when it comes to VR and AR operators, especially since the service they provide feels so different in many ways—so much more physical—than what the paradigm beneficiaries of § 230 offer. And haptic torts seem likely to be seen as not covered by § 230 at all.

\section{F. Tort liability for physical injury to users; terms of use as contractual limits on liability}

Finally, VR and AR defects are likely to also lead to injury to the systems' own users. Here, the analysis will be much the same as in the previous subsection, but subject to any enforceable terms of use that might waive liability to the users themselves.

Those limits, though, are likely to be substantial. The ubiquity of "consent" to terms of use may mean we will see relatively few VR and AR legal disputes brought by users in the courts. Unlike in Part II.E, here we mean not informed consent to having someone hit you with a virtual sword, but the fictional consent we consumers give whenever we are held to have agreed to terms of use that exist somewhere in a box or on a web page.\textsuperscript{146}

All the VR and AR legal issues we have discussed are likely to arise, at least in the foreseeable future, in the context of private, proprietary systems. Everything you do in VR—both personal experiences in your own home and interactions with others—occurs in a computer environment that is privately designed, recorded, and controlled. The same is true for the overlays that AR provides over your experience of the real world. For that reason, they are likely to be covered by the VR and AR operators' terms of use.

It is too soon to know exactly what this will mean for the law of VR and AR. But we have some experience with so-called "walled gardens" in


electronic communications. And that experience suggests that makers of the platforms have almost plenary authority to do what they want without legal complaint from their customers, at least when it doesn’t involve physical injury.

That is particularly true when it comes to potential economic loss. Users of Apple phones, for instance, have access to the public internet and phone networks but are at the whim of Apple’s decisions of what apps they can and cannot run. Apps can be dropped from the store, and if they are, users lose any investment they made using the app. Players of massively multiplayer online role-playing games (MMORPGs) invest substantial time and resources in creating and leveling up avatars and accumulating resources—but that investment exists only so long as the game remains live, and only so long as the company doesn’t boot the player off the system.

Waivers of liability would likely also likely cover injuries to privacy or other emotional distress. If a VR or AR operation wanted to disclaim any liability stemming from indecent exposure, virtual grooping, and the like, it could do so. The question whether such operators are hypothetically liable under some negligent supervision or entrustment theory, or have 47 U.S.C. § 230, may thus prove to be largely moot.

You are also likely bound by the terms of use even when you haven’t read them, and thus haven’t agreed to them in any normal sense of the

---


148 Lastowka & Hunter, Virtual Crimes, supra note 105.

149 Apple periodically bans apps for actual or perceived violations of its terms of service, or sometimes for no (disclosed) reason at all. See Lucy Black, Dash—Life Without the App Store, Feb. 24, 2017, http://www.i-programmer.info/news/201-ios/10547-dash-life-without-the-app-store.html ("Kapeli Dash was summarily removed by Apple with no prior warning. . . . This is by no means an isolated incident—Apple’s decisions are generally final, even when they seem harsh or even unfounded."); Sarah Perez, Controversial Crime Reporting App Vigilante Banned From App Store, Nov. 2, 2016, https://techcrunch.com/2016/11/02/controversial-crime-reporting-app-vigilante-banned-from-app-store/.


152 While the user might not be the person who bought the system, that likely won’t matter. Putting on the headset is likely to be treated as agreeing to terms of use by most modern courts. See, e.g., NANCY S. KIM, WRAP CONTRACTS (2014); Mark A. Lemley, Terms of Use, 91 MINN. L. REV. 459 (2006)
word.153 And precisely because those terms are not negotiated or read, they tend to give the companies that write them lots of rights and few responsibilities.154

The ubiquity of terms of use is not new, of course. The same problem infects web sites. But the effect of those terms is likely to be greater in VR and AR than it is in web site visits. VR systems are likely to collect not just data about you but other sensitive information, particularly if (as seems likely) one early use of VR is for virtual sex. And as we have seen, the importance of consent to physical contact and other behavior is likely to be much greater in VR and AR than it is in web site visits.

VR and AR may thus represent the acceleration of a trend begun with the Internet: the tendency of contract law to swallow property and tort law. Unless the law changes, VR and AR legal obligations (or their absence) will likely be determined mostly by the dictates of contracts written by VR and AR companies.

VR and AR operators’ liability for negligent physical injury or even negligent property damage, though, may not be as easily waived. Many states are less likely to enforce waivers that are part of nonnegotiable form contracts.155 Many are also less likely to enforce waivers when an activity is seen as practically necessary—not just if it’s medical care, but possibly also auto repair156—rather than just as entertainment.

VR and AR might at first seem like a form of recreation, which may cut in favor of enforcing the waivers.157 But as they become more important for employment and business, they may indeed come to be seen as practical necessities.158 So perhaps in the comparatively rare situations where physical injury is possible in VR and AR, and the provider is seen as negligent for not taking reasonable steps to prevent the inju-

153 *Id.*
156 See, e.g., Tunkl v. Regents, 383 P.2d 441 (Cal. 1963) (holding a waiver of negligence liability as to medical care, even charitable care, unenforceable).
157 See, e.g., Randas v. YMCA of Metro. L.A., 17 Cal. App. 4th 158 (1993) (holding a waiver of negligence liability in a swimming class to be enforceable). *But see* City of Santa Barbara v. Superior Ct., 161 P.3d 1095 (Cal. 2007) (holding a waiver of gross negligence liability to be unenforceable even as to recreational activity).
158 See, e.g., Gardner v. Downtown Porsche Audi, 180 Cal. App. 3d 713 (1986) (holding a waiver of negligence liability in a contract with a car repair shop unenforceable, when the shop’s negligence allowed the car to be stolen).
ry, the waiver that the provider requires users to sign might be ineffective.

G. Copyright and trademark liability to outsiders

Let us now turn to liability that isn’t preempted by terms of use (because it involves the rights of people who aren’t themselves VR or AR users), and is expressly exempted from 47 U.S.C. § 230 immunity: liability for copyright and trademark infringement.

Say that you are designing your own avatar. You could make it look as much like yourself as possible, receding hairline, love handles, and all.\(^\text{159}\) But, as we mentioned above, one of the exciting things about VR is the malleability of your identity. Why not make yourself just a bit younger and more attractive? Or change your hair color?

For that matter, why not experiment with a different race, or gender, or species? Freed of biology, and of the need for permanence, people will experiment with all kinds of images to represent themselves. And while some will try to create something new, some will just copy. Why not look like ... Superman? Lara Croft? The Cat in the Hat?

Copyright and trademark lawsuits against VR/AR users who create such avatars, or companies that sell them, would likely operate much as they have now, though with many of the uncertainties we see now. Fictional characters’ images coupled with their unusual character traits are protected by copyright. If you copy enough of the visuals, character traits, or both to be copying expression and not just idea, you might be infringing. What if you just wear a red-and-blue superhero costume with a cape but no S? What if the game lets you have certain superpowers, and you also have your character appear and disappear by appearing to fly?\(^\text{160}\) Answering questions like that is why IP lawyers get paid the big bucks.

If your use is noncommercial, and licensed avatars aren’t already being distributed by the copyright owner, your use might be a fair use. But if someone goes into business selling such avatars without the copy-

---

\(^{159}\) Well, for some of us, anyway.

right owner’s approval, such a use would probably not be a fair use. It might also be trademark infringement.

Copyright and trademark owners, though, might well not want to go after individual users, or even small-time fly-by-night avatar sellers. Instead, they might sue the VR or AR operators as contributory infringers. The environment operator might be immune under the Digital Millennium Copyright Act, but only until someone sends the operator a notice-and-takedown request; and then the operator would have to promptly block the allegedly infringing avatar, or risk losing a lawsuit.

There is an established body of case law that sets out the limits of intermediary liability under the DMCA. There is less clarity on intermediary liability for trademark infringement on the Internet, but there too the law is developing. But the legal issues—and their practical consequences—may differ somewhat in the VR and AR environments.

First, while there are certainly opportunities for outright copying of works or logos in VR, we expect that many of the allegations will be against user-generated works that incorporate or modify those works, particularly copyrighted works, rather than wholesale duplication of the kind that is common online. Those user-generated works can still be infringing, but they are more likely to be transformative and less likely to be commercial, complicating the copyright case and raising the likelihood of overzealous enforcement by copyright owners.

Second, the use of AR is likely to generate some novel copyright issues involving derivative works. One way to infringe copyright is to combine your work with another in a way that creates a new work or changes the market for that work. AR users may do exactly that whenever they place a virtual Pokemon “in” a work of sculpture, visually merge the copyrighted work that appears in their phone or glasses with

---

163 See, e.g., Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012).
164 See, e.g., Tiffany (NJ) Inc. v. eBay Inc., 600 F.3d 93 (2d Cir. 2010); Mark A. Lemley, Rationalizing Internet Safe Harbors, 6 J. TELECOM. & HIGH TECH. L. 101 (2007).
an actual work that appears in front of them, or use filters that alter the appearance of copyrighted works.

True, those new derivative works are just passing things, not permanent alterations, at least unless the user takes a photo. But some case law has treated such ephemeral changes to a copyrighted work as infringing. Courts will have to decide whether and under what circumstances a user’s subjective viewing of a derivative work not visible to others—or the facilitation of such an act—constitutes copyright infringement.

Finally, the consequences of copyright infringement under the DMCA may be more significant for the infringer in VR than on the Internet. To comply with the DMCA, intermediaries must agree to take down identified acts of infringement and to terminate the accounts of repeat infringers. On the Internet, neither penalty is all that drastic—or all that effective if you are a copyright owner. It is easy enough to repost a video that has been taken down, and frequently not that hard to create another account from which to do so.

But it is harder to know what it means to “take down” a VR avatar that infringes copyright or trademark law, so companies may err on the side of caution by deleting the account altogether. And we think people will be more invested in their VR accounts than in a particular online account with a particular web site, so the consequences of VR infringement under the DMCA may turn out to be higher than on the Internet.

IV. HOW OTHER PEOPLE SEE YOU, EVEN IF YOU DON’T SEE IT

A. Your role in others’ personal sensescapes

So far, we have spoken of intrusions on VR or AR users’ own sensescapes—actions that cause them to see, hear, or feel things that are offensive or even harmful to them. But what if other users decide to include you in their sensescape, even in ways that you might not directly perceive?

Our inclination is towards what we call “freedom of sensescape”: People should generally be free to see and hear whatever they want in their own VR displays, even when the material is offensive or may lead some people to behave badly. (We would say the same as to AR, except for rules aimed at preventing distracted driving and the like.) The contents of one’s own VR sensory feed are very close to the contents of one’s thoughts and fantasies. Banning people from displaying VR images to

166 See, e.g., Lewis Galoob Toys, Inc. v. Nintendo of America, Inc., 964 F.2d 965 (9th Cir. 1992); Atari, Inc. v. North American Philips Consumer Electronics Corp., 672 F.2d 607 (7th Cir. 1982); Micro Star v. Formgen Inc., 154 F.3d 1107 (9th Cir. 1998).

themselves simply because it offends others (even the subjects of the images), or may lead to bad behavior, should be as improper as trying to punish people for unexpressed fantasies, or for notes written in their own diaries.

But what if my sensescape offends you, because it refers to you in certain ways, even if you don’t personally experience it? We suggested earlier that users can engage in self-help by turning down your volume if you are too loud, virtually clothing your avatar as it appears on their AR or VR display, or keeping you out of their personal space, all without your consent or perhaps even your knowledge, merely by changing their local software setting. But if the software provides such control, it won’t always be used to prevent crimes or torts.

What if people instead make your avatar appear naked to their eyes without your knowledge or consent? Naturally, they probably won’t be able to make it look like your naked body actually looks, unless they have some photographs of your naked body. But they can just merge your face and your gestures and motions with a generic computer-generated naked body tailored to your physique and skin tone.

Or what if your “personal space” bubble prevents you from perceiving other avatars as groping you, but they can still see themselves groping you? True, software companies might design a system in such a way that all parties had to share a common visual version of events. But there’s no guarantee that this is the way systems will indeed be designed, and some reason to think that software companies would want to give each user more flexibility. For instance, if you and we go to a VR bar together, why not let each of us perceive the décor of the bar in the way that we most like, for instance if you like a loud dark crowded bar and we like a quiet well-lit uncrowded one?

What’s more, in AR, all this can happen when the people are physically right next to each other. If they can load a software program onto their glasses that reminds them of your name and your kids’ names while talking to you at a cocktail party, what if they instead load your most embarrassing picture from a social media site while looking at you, or a fake “nude” image of you?

From one perspective, we might react by saying, “you can’t see the naked person or the groper; problem solved.” You are not confronted with something that offends you or that you perceive as an assault, so you do not suffer injury.

---

168 See supra Part II.A.2.

169 Fake celebrity porn—photoshopping someone’s head onto an image of a naked body—is a real thing. This one too you can look up for yourself if you really want to.
It’s creepy if you find out about this later, or if you see signs that this is happening right now. But “creepy” doesn’t mean illegal. No law, for instance, prevents someone in the privacy of their own home from masturbating while thinking about you or looking at your picture, even if you really don’t want them to.\textsuperscript{170}

On the other hand, you may well be upset when you learn that you are being viewed (here, literally viewed) disrespectfully. And this might especially trouble you when you are in virtual or real personal proximity to the people who are viewing you that way: People who are (in their subjective experience) virtually ogling or groping you may treat you differently in that interaction—physical interaction when it comes to AR, virtual interaction in VR—than if they weren’t doing so.

Of course, if this is just what people themselves see in their individual headsets, no one will be the wiser. But information about how they’ve configured their systems might come out, whether through discovery in litigation, a search under a warrant, or a hack. And even if it doesn’t, the possibility that people are doing this may affect how we interact with others in VR, or even in the physical world with people who are wearing AR.

This creepiness may well be reason for companies to ban or restrict some kinds of perception. But we don’t think it makes such behavior illegal. That is true even for otherwise unprotected speech. Possessing child pornography depicting actual children may be banned, the Supreme Court said, because the possession itself stimulates a market for the creation of the speech, creation that involves criminal harm to the children. But display of speech that was not created as a result of criminal conduct is protected.\textsuperscript{171}

Indeed, the Supreme Court’s \textit{Stanley v. Georgia} decision, which held that mere possession of obscenity cannot be punished, fits well with this principle:

Whatever may be the justifications for other statutes regulating obscenity, we do not think they reach into the privacy of one’s own home. If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch. Our whole constitutional heritage rebels at the thought of giving government the power to control men’s minds.\textsuperscript{172}

That is even more apt, we think, for the contents of one’s VR display. And the law of disclosure of private facts, false light invasion of privacy, and the right of publicity fits the freedom of sensescape as well: Those

\textsuperscript{170} We’re not personally at much risk of this, but we understand others might be.


\textsuperscript{172} 394 U.S. 557, 565 (1969).
torts don’t even apply to material shared with a few friends, and even more clearly don’t apply to material displayed for one’s own benefit. 173

None of this is to say we shouldn’t be bothered by this sort of conduct. VR and AR companies may want to ban or restrict it, or at least to warn people that it is (or might be) happening. Our point is only that it isn’t illegal.

B. Display to others

Now let’s take a step away from purely individual decisions to view another’s avatar differently. Say that John decides to configure his own VR system to substitute a different avatar for your own when he sees you in VR; but say that he also shares this with Jack, Jerry, and Jane. And say that avatar is in some way disrespectful.

Maybe John thinks that you are a fascist and decides to draw a little Hitler moustache on you, or put a swastika armband on his image of your avatar; and all his friends then copy that design. Indeed, maybe John announces to the world that this substitution is available to anyone who wants it (assuming the VR/AR environment makes it easy for people to do that). John might view that as a political statement, and so might the people who copy from him.

If you’re of our generation, think back to the Doonesbury cartoons that constantly represented Dan Quayle as a feather, Bill Clinton as a waffle, and Arnold Schwarzenegger as a giant groping hand. What if VR and AR users could do the same, not just in their sensescapes, but in the sensescapes of others who were willing to follow the user’s lead?

And what can be done for political reasons can also be done out of personal spite or cruel humor. John could share with his friends an avatar that is a grotesque caricature of an acquaintance’s (say, Alan’s) appearance, perhaps exaggerating some unattractive feature of Alan’s. Or John could share with his friends an avatar of their acquaintance Alice apparently naked, which is to say Alice’s face merged with a plausible-looking naked body.

Human nature being what it is, we expect there to be a good deal of this sort of behavior. And while much of it would be sophomoric, we think that on balance it should be protected by the First Amendment, especially since it can be used for political, social, religious, and artistic commentary.

One question is whether publicizing sexually themed adaptations of others’ avatars—an avatar that is configured to look like the user naked, even when the user has not chosen this—should be treated differ-

173 See Restatement (Second) of Torts § 652D cmt. a. Libel law also doesn’t apply when the speaker displays material solely for his own benefit. See Restatement (Second) of Torts § 577(1).
ently. Should such nonconsensual sexualization of others’ images be forbidden by law, by analogy to the recent movement to forbid to nonconsensual distribution of real sexual images (often labeled “revenge porn”)? Or does the fact that everyone understands the nudity to be faked lead the image to retain its First Amendment protection? Courts are beginning to litigate this question in the context of fake celebrity porn, though those cases are surprisingly rare, perhaps because none of the victims want to call more attention to the offending sites, or perhaps because the defendants are probably judgment proof, or in Bangladesh.

On the legal merits, privacy torts like “false light” invasion of privacy (if the images are fake), defamation (if they are fake but are presented as real), or public disclosure of private facts (if the image is real) all seem plausible responses to fake celebrity porn. But in VR, presumably no one thinks your naked avatar is “real”—it is, after all, an avatar. That makes these tort theories, focused as they are on factual assertions, much tougher to sustain.

C. Pervasive display

So far, we’ve talked about how you choose to alter others’ avatars. But what if you are designing your own avatar, and you deliberately choose someone else’s name and appearance, perhaps to mock that other person, or perhaps to impersonate them?

Say that someone creates an avatar in a popular VR environment. He calls the avatar Eugene Volokh (or Mark Lemley), and he makes it look like Eugene Volokh. (Recall that we’re assuming avatars that are highly lifelike, something that will likely arrive within the next few years.) Then this “Eugene Volokh” starts traipsing through the VR environment, saying and doing all sorts of foolish things.

Now maybe we could sue for libel, or even seek criminal punishment under various state laws that ban impersonation. But say that it’s clear that this isn’t the real Eugene Volokh; for instance, say that the VR world has a special marker for people who are admittedly pseudonymous (e.g., by displaying a scarlet P for “pseudonym” on the front of

---


177 See, e.g., People v. Golb, 23 N.Y.3d 455 (2014).
their avatars). Reasonable observers would therefore realize, on a moment’s reflection, that this isn’t the real Eugene Volokh.

If this were a movie, then this use of a real person as a character, as in *Forrest Gump* or *Midnight in Paris*, would be permissible, even protected under the First Amendment, notwithstanding any possible “right of publicity” claim. It might be parody, or a fictionalized account of real events, or just entertainment, humorous or not. But so long as a reasonable person would perceive it as something fictional, rather than as making factual assertions about the real person, it wouldn’t be actionable, either as libel, false light invasion of privacy, or infringement of the right of publicity.

By the same logic, it may well be that designing an avatar that uses the name and likeness of a real person as an obviously fictional character in a VR or AR environment should likewise be permissible. This may indeed be the right answer, and there is real value in such a conclusion. Letting people play others online, especially when it’s clear that this is just a pseudonym, can be a useful means of parody, commentary, and entertainment.

But perhaps such avatar design should not be allowed unless the person whose name and likeness is used consents, because the visceral quality of VR might make a difference. If you see a movie with a Eugene Volokh character, you don’t just know you’re seeing a movie—you feel that you’re seeing a movie. You’re sitting in your armchair, with the movie visibly on a screen in front of you. You have a popcorn bucket in your hand, or a snack on the coffee table. You probably see other viewers in front of you or beside you.

But if you see an avatar in a VR world, you’re seeing it in a context specially designed to mimic reality as much as possible. When you turn your head, the illusion created by VR is reinforced, not broken. In more advanced VR systems, you might be walking around on a two-dimensional treadmill rather than just sitting in your armchair.

Moreover, you’ll see the avatar not in some special context that you bring up just to see impersonations (e.g., a Saturday Night Live broadcast). Rather, you might see the avatar in your ordinary “travels” in the VR environment. Even if you logically recognize that the avatar is a pseudonym, it will feel like a person named “Eugene Volokh.” And you might see the avatar fairly often, if he goes to the same on-line conferences or chat rooms or bars that you frequent.

---

The danger, then, is that your experience of the fictional “Eugene Volokh” will color your perception of the real Eugene Volokh. Even if you intellectually know that the dumb or rude things that “Eugene Volokh” says weren’t really said by the real Eugene Volokh, when you actually meet the real Eugene Volokh those things may still taint your view of him. Perhaps you won’t take what he says as seriously. Or perhaps you’ll work hard to try to put the fake “Eugene Volokh” out of your mind while interacting with the real one, but that very process will distract you from your real interaction.

This, of course, is much like the concern that animates the law of trademark dilution by tarnishment. The law prevents people from producing Dogiva dog biscuits, even when consumers won’t likely be confused into thinking that the dog biscuits are really from the people who make Godiva Chocolates. It’s enough that the dog biscuits might taint the associations of the chocolates, and may make the chocolates less appetizing.

To be sure, trademark dilution law is limited to commercial uses; the use here is noncommercial, and perhaps that should be relevant. Moreover, trademark dilution law is limited to “famous marks,” ones widely recognized by the general consuming public of the United States. Our concern is actually with the opposite. If there is an avatar who is named “Justin Bieber,” and who looks like Justin Bieber, this probably won’t color your perception of the real Justin Bieber: You’re more likely to viscerally perceive the avatar as just a pseudonym, and because your mental image of Justin Bieber is going to be more molded by Bieber’s much larger media presence. Rather, our concern is for people who aren’t particularly famous; they are the ones whose identity is most likely to be diluted by avatar impersonation.

If this argument is right, then perhaps the right of publicity should have a broader scope as to VR and AR avatars than in other contexts, including as to noncommercial uses. Or perhaps we should be satisfied with some form of labeling, in much the way we distinguish “Real Donald Trump” from other Donald Trumps on Twitter by using a blue verified check mark.

---

179 See, e.g., 15 U.S.C. § 1125(c); CAL. BUS. & PROF. CODE § 14202.
182 Some have likewise suggested that truly famous names and marks are actually hard to dilute. See, e.g., Louis Vuitton Malletier v. Haute Diggity Dog, 507 F.3d 252, 267 (4th Cir. 2007);
183 Though the right of publicity is generally applied just to commercial uses, some older cases suggest that even noncommercial appropriation of another’s name or likeness might sometimes be actionable. See RESTATEMENT (SECOND) OF TORTS § 652C cmt. b.
We are inclined to be cautious in expanding both the right of publicity and the trademark dilution theory. The right of publicity has generally to exclude noncommercial uses, and we think that this is no balance an important safeguard. The scholarship on dilution is at best inconsistent, and we have argued elsewhere that dilution law, like right of publicity law, raises significant First Amendment concerns. But at a minimum the visceral nature of VR presents an interesting test of the theory of tarnishment; and as we learn more about how VR is actually experienced, we might find that our views have to change.

V. Pervasive Information Capture

Finally, the fact that these contracts will vest rights with the hardware and software providers compounds another significant aspect of VR: because it is all software that captures your motion and activities and responds to them, there is a record of everything you do in VR. That record likely exists not only on your computer but also in the cloud. The company probably has broad access to it under the terms of use. VR companies might or might not store it depending on space and legal constraints.

True, such pervasive information capture happens with your Internet browsing habits and data on your smartphone. The devices and sites you use track and store more than you think. But the data needed to make VR and AR work must not only generate a record of where I am and whom I interact with at any given time, but may also save records of intimate acts and conversations. And the visceral, visual nature of those records may make us more concerned about the privacy of those records than we are about most of our texts.

Indeed, this sort of retention might be billed as a valuable feature for users, who can then have a “life log” that they could review or search later to refresh their memories or relive or show others interesting moments. But it may happen even when users would rather that it didn’t happen, especially when it comes to their interactions with others who do choose to keep such life logs.

And the retention might also be useful for in-system dispute resolution systems, for instance if users dispute the terms of a commercial transaction they entered into online, or claim that they were libeled or


otherwise injured. Perhaps there might be, for instance, a form of internal subpoena, where people can require the production of any conversations that involved them. That offers the promise of helping resolve many of the kinds of disputes we discussed above, either by providing evidence in court or by facilitating dispute resolution outside the legal system.

Maintaining such records, though, will also facilitate government investigations in circumstances in which the law does seek to intervene. That will sometimes be good. But it can also be abused. Presumably all such recordings would be subject to subpoena—but only if they’re kept in the first place. Should they be? Under current Fourth Amendment law there is no constitutional barrier to such subpoenas or even outright searches (on the theory that one can’t have a strong expectation of privacy in data one turns over to VR and AR companies). But should there be some sort of privilege, developed by common law or by statute, either requiring a high showing of relevance for such subpoenas, or perhaps even categorically banning them (as would be the case for most attorney-client-privileged or priest-penitent-privileged information, for example)?

VR and AR operators need to consider all these questions, and VR and AR users need to consider what they want, especially if different operators adopt different policies. How long should the systems maintain records of in-system interactions? Should they let individual users erase their own records? What records should be kept for possible future dispute resolution? And the legal system needs to consider how broadly such records should be made available to the government and to litigants.

To be sure, there may be practical limits to data capture. VR generates a lot of data—too much to practically transmit and store on an ongoing basis, at least today. That fact might itself mean that while everything that happens in VR generates data, we may not keep much of that data for very long. But perhaps as storage gets ever cheaper and quicker, even that will not be a barrier.

VI. CONCLUSION: THE LIGHT VR AND AR CAN SHED ON LEGAL DEBATES MORE BROADLY

As promised, we have just sketched some of the more interesting legal issues that VR and AR are likely to generate. But some of this anal-

---

187 Some have argued that there should be a warrant required in such cases. See, e.g., Jonathan Mayer, Constitutional Malware, ___ YALE L.J. ___ (forthcoming 2017).

188 See, e.g., United States v. Jean, 2016 WL 4771096 (W.D. Ark. Sept. 13, 2016) (summarizing caselaw on the limits to Fourth Amendment protection in material that users communicate to computer service providers).
ysis, we hope, can also reflect on broader legal debates. Let’s briefly recap some such possibilities.

A. Order without (much) law

For various reasons, we might see crimes, torts, and other problems arise in VR without the legal system doing much about it. The Bangladeshi problem will mean that enforcement will often be too difficult, especially as to the less serious crimes and torts that we’re likely to see in VR and AR. The availability of technologically enabled self-help will give people a cheap alternative to calling the police and going to court, and will in turn make police even more reluctant to intervene. VR and AR operators’ ability to contractually waive liability, coupled with 47 U.S.C. § 230, will likely discourage lawsuits against the operators.

And this relatively lack of government-imposed law may not be bad. There is a natural tendency for legislatures or courts to intervene to try to solve perceived problems with new technologies. But the best way to nurture a new technology can sometimes be for the law to leave it alone.

Anupam Chander has argued that a series of (largely accidental) decisions in the early history of the Internet created safe spaces in which companies could innovate without the fear of government regulation. The same may prove true of VR and AR. We don’t yet know how these technologies will develop, both technologically and culturally. Setting legal rules too early risks rendering those rules irrelevant as the technology moves in unexpected ways. Worse, legal rules can channel or stifle the development of technology. So a generally hands-off approach to regulation of VR and AR is probably good, at least for now.

At the same time, many of the problems we discussed above are (or are likely to become) real ones. In the absence of legal regulation, VR and AR communities can and should develop their own norms to govern permissible and impermissible social interactions. VR and AR companies (both hardware platforms and software companies) can also contribute by considering and adopting best practices for behavior. Operators could set up dispute resolution systems within the environment they run, whether for quality-of-life matters or for commercial transactions.


There are, however, limits to private ordering as a solution to disputes that arise in VR and AR. We are likely to see those limits tested when operators seek to insulate themselves completely from liability for any sort of injury (as they invariably will). Many of the potential harms involve the risk of physical or at least serious psychological injury. That makes it important that consent at least be a real thing, not merely a conclusion that somewhere there is a terms of service contract posted and I am deemed to have agreed to it by turning my machine on.\textsuperscript{191}

There is a good argument that courts have stretched the definition of consent too far in the browsewrap cases generally.\textsuperscript{192} But even if contract law continues to enforce these terms in general, courts are increasingly pushing back on specific provisions that seem unfair or surprising to consumers and that are contained in contract forms the consumer had no effective opportunity to review.\textsuperscript{193} Consent should mean informed consent, not simply a legal acknowledgement of the existence of boilerplate somewhere. And in the real world even clear waivers of liability often don’t apply to negligent or intentional physical harm.\textsuperscript{194}

\textbf{B. Virtual reality and the speech-conduct distinction}

VR and AR will also challenge our understanding of what is speech (or, more precisely, communication)—and thus strongly protected by the First Amendment and other norms—and what is nonspeech conduct that merits regulation. Is a nude avatar like nudity on a drive-in screen (speech) or like indecent exposure (conduct)? Are avatars apparently having sex like a sex scene on a drive-in screen (speech, though perhaps in some situations within the obscenity exception) or public lewdness (conduct, and indeed a sex crime)?

Is virtual non-haptic groping like the display of an image (speech) or like unwanted touching, or the threat of unwanted touching (conduct)? Is the display of a scene that leads the user to walk off a cliff, or even just into his apartment wall, more like an error in the Mushroom Encyclopedia (speech) or an error in an aviation chart (treated by the law as conduct)?

There are good reasons in the physical world to distinguish between words and actions and between words and things. Some of the lines turn

\textsuperscript{191} Joshua Fairfield argues that terms of use contracts cannot suffice to create legal rules for virtual worlds; we need some public law in those worlds. Joshua Fairfield, \textit{Anti-Social Contracts}, supra note 146.

\textsuperscript{192} See, e.g., Kim, \textit{supra} note 152; Lemley, \textit{supra} note 152.

\textsuperscript{193} For recent efforts to rein in the reach of browsewrap contracts, see Nguyen v. Barnes & Noble, Inc., 763 F.3d 1171 (9th Cir. 2014); Specht v. Netscape Comm’sns Corp., 306 F.3d 17 (2d Cir. 2002); Meyer v. Kalanick, \textit{supra} note 152, 2016 WL 4073012 (S.D.N.Y. July 29, 2016); Muhammed v. Uber Techs., 109 F. Supp. 3d 1185 (N.D. Cal. 2015).

\textsuperscript{194} See \textit{supra} notes 156 & 158.
out to be difficult to draw, and some of the results might not make a whole lot of sense. But the basic distinction makes sense in the physical world because we think the harm words can cause at a distance is generally less (and easier to avoid) than the harm of physical contact.

VR and AR, though, are deliberately created to make communicated images and sounds feel like real life. The technologies challenge our perception of the real because they blur the cognitive line between imagery and physical presence. People react to a virtual slap as if they had actually been slapped.\textsuperscript{195} The reaction is visceral; it doesn’t involve real physical contact, but it feels real in a way.

That requires us to consider why we restrict things like indecent exposure when we don’t restrain images of the same things, and whether the physical reality or the perception should be the driving force.\textsuperscript{196} And that in turn raises fundamental questions about what counts as harm, in VR and AR or outside it.

\textbf{C. The virtual, the real, and the nature of harm}

The self-help options we discussed above, unlike systemic limitations on what can happen, change only my lived experience and not yours. If I exercise the option to avoid seeing you naked, you may not know about it. As far as you know you’re naked in front of me, but my experience is that you are clothed.

We might be fine, even happy, with that difference. It allows a sort of live-and-let-live freedom of sensescape in which our vision of what happens differs. We might even think that if freedom of sensescape should be a baseline legal norm of VR, it will often require that different people perceive things differently.

But maybe that shouldn’t satisfy us. Does the ability to prevent my perception of bad things mean that they don’t injure me? That turns out to be a hard question that gets at some pretty fundamental issues around the nature of harm. If the harm is my physical or psychological experience of seeing you naked (or being virtually groped), much and perhaps all such harm can easily be avoided by giving me control over how you appear to me and how you can interact with my avatar.\textsuperscript{197}

\begin{footnotes}
\item[195] See supra Part I.C.2.
\item[196] For a similar discussion of whether Internet law should consider the way the Internet actually works or the way it seems to users to work, see Orin Kerr, \textit{The Problem of Perspective in Internet Law}, 91 Geo. L.J. 357 (2003).
\item[197] The exceptions will be things like defamation, fraud, and the right of publicity, because they affect how I am viewed by third parties. My reputation is injured by your defamation even if I never learn about it. Indeed, the harm
\end{footnotes}
But maybe we should still be worried about even second-party perception. If I can superimpose clothes on your naked avatar, you can presumably do the opposite, viewing me as naked even when I am subjectively wearing clothes, or making me appear to you as Donald Trump or Hillary Clinton. You probably find that creepy in VR. It will be even creepier when it happens in AR. Similarly, even if I have a personal bubble in which you can’t grope me—from my perspective—you might be subjectively experiencing a world in which you are groing me.

We might worry that this subjective or unshared experience will have corrosive effects on the real world. If you perceive me as naked when you are talking to me you are likely to treat me differently in that conversation, and perhaps treat me differently afterwards. It is not clear that the law should, or even can, regulate that behavior. But perhaps we should worry about the effects of that behavior as a society.

This in turn requires us to think seriously about some distinctions we take for granted—between presence and remoteness, between speech and conduct, and between what is real and what is “merely” perceived. If it turns out that the reason we ban indecent exposure is in part about perception and psychic harm rather than physical threat, that might cause us to rethink what it means to be hurt in a way the law cares about. If it turns out that we care about the perpetrator’s subjective perception of reality, not just the victim’s, that suggests a much broader notion of what we would punish if we only knew about it. And that has implications not just for the virtual world but also for the real world.

We don’t have definitive answers to these questions. But the very existence of VR and AR poses the questions in new ways, ways that can illumine the assumptions the law makes about freedom and harm in the physical world as well as the virtual world. For that reason alone, it is worth paying attention to the developing law of virtual and augmented reality.
Security firm claims implantable cardiac devices can be hacked

By Ryan Whitwam (https://www.extremetech.com/author/rwhitwam) on October 24, 2016 at 4:45 pm
4 Comments (https://www.extremetech.com/extreme/238161-security-firm-claims-implantable-cardiac-devices-can-be-hacked#disqus_thread)

As more and more devices gain connectivity, there are more opportunities for malicious individuals to steal your data, break things, and just generally make your life more difficult (http://www.extremetech.com/internet/238042-internet-struck-by-waves-of-outages-as-massive-ddos-attack-affects-major-services). At least you'll still have your life, though. Now a security firm says that a connected implantable cardiac device made by Minnesota-based healthcare company St. Jude is susceptible to hacking (https://www.extremetech.com/tag/hacking), which can be life-threatening.
The device at issue here is an Implantable Cardioverter Defibrillator (ICD). This is essentially a more advanced version of a pacemaker. After implantation, it uses small flexible wires to detect your heart rate and applies an electric current to stop abnormal cardiac rhythms. An investment firm called Muddy Waters started warning about the safety of St. Jude’s ICD products recently, which has led to a legal battle. Muddy Waters is a short-selling operation, meaning it bets on a company’s stock price falling in order to make money. St. Jude says the allegation of security issues is simply meant to harm its stock price and is not based on a real danger.

As part of the ongoing case, Muddy Waters contracted with cyber security firm Bishop Fox to perform an independent analysis of St. Jude’s implantable cardiac devices. It recently produced a 53-page report where it says Muddy Waters’ claims regarding the possibility of ICD cyber attacks are “by and large accurate.”

St. Jude’s latest medical implants are different from past devices because they use a wireless protocol to communicate with a monitoring station called Merlin@home. It uses radio frequency signals to transmit and receive data from the implant, which saves patients from going to the doctor several times per year just to have the implant’s performance checked. However, Bishop Fox says it successfully hijacked this signal and was able to take control of the implant.
At a distance of 10 feet, researchers claim they were able to instruct the ICD to cease operation, then produce a powerful T-wave shock. A patient subjected to this attack could have a heart attack. That’s somewhat worse than having your family photos locked up by ransomware. Bishop Fox says it believes the same attack could be accomplished from as far as 100 feet away with more powerful equipment.

The claims are currently being investigated by St. Jude and the FDA, but the federal agency said patients should continue using their ICDs as instructed by doctors. If this turns out to be a real threat, the fix is going to be costly. It’s harder to recall defective electronics when they live inside your chest.
We-Vibe sex toy manufacturer settles US class action for almost $4 million

Lucy Cormack

The manufacturer of a bluetooth-enabled sex toy has reached a US class action settlement of almost $4 million, after it was found to be collecting intimate data about the way purchasers used the vibrator device.

The class action against sex toy company Standard Innovation Corporation was brought in the federal court by two anonymous women in the US last year, in relation to the We-Vibe 4 Plus, a product advertised as the "No. 1 couples vibrator."

The prime feature of the device allows users to adjust intensity and vibration patterns using a smartphone linked to the 'We-Connect' app, enabling couples to "play together even when [they're] apart".
Internet capabilities of the We-Vibe product line allow devices to be controlled long distance, for example between two people on opposite sides of the globe. Individual We-Vibe devices retail in Australia for between $170 and $300.

However in September last year it was revealed that intimate data from the device was being regularly sent back to the manufacturer when in use.

Such data included pattern and intensity levels of vibrations, the device's temperature, when it was used and for how long, and the email address of customers registered with the device's app.

Spokesman for Standard Innovation Denny Alexander said the information was stored to help "improve products and for diagnostic purposes".

"The data was used only in aggregate, non-identifiable forms," he told Fairfax Media.

The lawsuit against the manufacturer alleged that it was "intercepting and monitoring electronic communications between a user's smartphone and the device, and then collecting and transmitting this data to servers in Canada," (where the company is based).

Court documents state that the settlement agreement "achieves the dual purposes of the suit by providing both significant monetary compensation and cessation of [Standard Innovation's] allegedly invasive information collection practices."

As part of the settlement, Standard Innovation was required to
As part of the settlement, Standard Innovation was required to establish two settlement classes: an 'app class,' for those who used the app and and a 'purchaser class,' for those who only purchased and used the device.

According to court documents, about 300,000 people purchased Bluetooth-enabled WeVibe products, while around one-third of those also used the app.

The settlement entitles any person who purchased the vibrator to claim up to CAD$199, while anyone who actually connected the device to the app could receive up to CAD$10,000.

However it is expected that purchasers of the device will receive around $40, while others who also used the app will receive around $500.

Mr Alexander said the company was pleased it had reached a fair and reasonable settlement.

"At Standard Innovation we take customer privacy and data security seriously. In September this year, we responded rapidly to concerns about app privacy and security," he said.

"We enhanced our privacy notice, increased app security, provided customers more choice in the data they share, and we continue to work with leading privacy and security experts to improve the app."

Mr Alexander confirmed that while the settlement only applied to customers in the US, the company had made privacy and security updates on a global scale.

"Prior to September 2016, app users in all territories had the option of creating an account with their email address. This option has since been removed from the app."

Standard Innovation has agreed to delete all email addresses provided via registration, the time and date of use on any device, vibration intensity levels and patterns, device temperatures and battery life.

- Interact with us on Facebook - Savvy Consumer
- Latest consumer news
Privacy is pretty important when it comes to sex toys.

By Julia Malacoff | Mar 15, 2017

When you're using a vibrator, the last thing you're thinking about is the fact that it could be recording information about you, right? Unfortunately, last year, hackers revealed that the makers of We-Vibe vibrators were getting a little more intimate with their customer base than was originally thought. Turns out, they were collecting data about the users of their products, which understandably resulted in a class action suit against the company. Yikes! (Looking for something more subtle? Here are five vibrators disguised as everyday objects.)

The vibrators themselves are very popular since they have some pretty awesome couple-friendly features. The toys can be hooked up to an app that controls the devices from anywhere in the world, making them especially ideal for long-distance couples. The problem is that the makers of
the toys were using the corresponding app to collect data like time and date of use, frequency and duration of use, and settings used during each session. All that info, along with the email address of the person who was using the app to control the toy, was transferred back to the company's servers, logging it for market research purposes. It does make sense that a company would want to know about how often and in what ways people use its products, but the court ruled that violating people's privacy in order to do that wasn't the right move. Uh, maybe next time they'll just send out a customer survey? (If you're on the hunt for a new vibrator, these are the best vibrators for mind-blowing sex.)

The suit against the sex toy manufacturer was settled yesterday, according to the National Post, and luckily, the company has agreed to destroy all the information they've collected so far through the app and will stop collecting new information, effective immediately. Phew! But here's the craziest part: If you purchased a We-Vibe Rave before September 26, 2016, and you used the corresponding app, you're entitled to a $10,000 settlement. Yup, you read that right. If you didn't use the app but you purchased the product before that date, then you get $199.

FROM OUR SPONSORS

1 | Personalized Romantic Gifts
2 | Supplements for Skin Acne
3 | Foods for Clear Skin
4 | Hair Care Tips
5 | Best Skin Care Products
6 | Fat Burning Tablets

YOU MIGHT ALSO LIKE

The New Health Supplement That Doctors Are Taking
Sponsored | Observer

6 Weird Orgasm Conditions

Steamy Sex Positions to Try Tonight

After Hearing This Woman’s Horrifying Story, You’ll Never Pop Pimples Again
Privacy Policy

PRIVACY POLICY FOR SMARTBOD INCORPORATED, DBA LIONESS

Effective Date: May 1st, 2017
Last Updated: May 1st, 2017

Lioness is a registered trademark and trade name of SmartBod Incorporated. SmartBod Incorporated DBA/operating as Lioness is henceforth referred to as "Lioness" in this document, unless explicitly noted otherwise.

INTRODUCTION: OUR COMMITMENT TO PRIVACY

Your privacy is important to us. To better protect your privacy, we provide this notice explaining our information practices and the choices you can make about the way your information is collected and used. To make this notice easy to find, we make links available to it on our website, lioness.io, and at points where personal information may be requested.

This Privacy Policy applies to our vibrators and other devices ("Devices"), our websites, including but not limited to lioness.io (individually a "Site" and collectively "Sites"), the Lioness software ("Software") and Lioness mobile applications (the "Apps"). The Devices, Sites, Software and Apps are collectively referred to in this Policy as the "Lioness Service," and by proceeding to use the Lioness Service you consent that we may handle the data that we collect from you in accordance with this Privacy Policy.

This policy may change over time, but any future changes will not affect data that was collected under a previous version of this policy. Please check this page periodically for any changes. You may also be notified of the changes to our policy by email or any other method that Lioness
deems appropriate. Your continued use of the Lioness Service after being notified of the changes to our policy will constitute acceptance of our new Privacy Policy.

And remember, we're here to help. If something in this policy does not make sense or if you have any questions, please contact us at help@lioness.io.

YOUR CONSENT

By accepting Lioness’s Terms of Service (as a user of the Lioness Service) you explicitly consent to this Privacy Policy.

INFORMATION THAT YOU PROVIDE TO LIONESS

**Activate a Device**
When activating a Lioness Device, you will be asked to download the Lioness App or install Software and enter information about yourself. Depending upon the specific Device you use, your data may be collected and transmitted to Lioness.

**Create a Lioness Account**
If you want to access data collected by your Device, you must create a Lioness account. When you create a Lioness account, we ask for some personal information, including your email address, username, and password.

**Add Info to Your Account**
You can customize your Lioness experience by adding other types of information to your account, such as personalizing your profile with photos, participating in discussion boards, or sending messages. Whenever you add this type of data, we collect it and store it in your Lioness account.

**Visit Our Sites**
Lioness collects industry standard data from everyone who visits our Sites—even if you don’t have a Lioness account. This includes log data that automatically records information about your visit, such as your browser type, operating system, the URL of the page that referred you, the different actions you performed, and the IP address you used to access pages on the Site. We use this type of information to provide you with an experience that’s relevant to your location based on the IP address, to prevent Site misuse, and to ensure the Site is working properly. We also collect data from cookies.

**Sync Your Device**
When you sync your Device through an App or the Software, data recorded on your Device is transferred from your Device to our servers. This data is stored and used to provide the Lioness Service and is associated with your account. Each time a sync occurs, we log data about the
transmission. Some examples of the log data are the sync time and date, device battery level, and the IP address used when syncing.

Buy From Our Store
We do not view or store your credit card information. This is handled by our third-party payment processor. We store your shipping address so we can process your order through our fulfillment partner. If you are logged into your Lioness account when you purchase something on our Site, we associate that order with your Lioness account.

Contact Us
Whenever you contact Lioness for help, we collect your name and email address along with additional information you provide in your request so that we can provide you with assistance and improve the Lioness Service. This data does not expire, and is retained unless otherwise stated.

We only collect information about you when you're interacting with Lioness Products & Services.

WHY WE COLLECT DATA

Lioness uses your data to provide you with the best experience possible, to help you learn about your body, and to improve and protect the Lioness Service. Here are some examples:

- Contact information is used to send you notifications and to inform you about new features or products we think you would be interested in. Please see "Can I Opt-out Of Receiving Lioness Emails?" for information on how you can opt-out of future communications.
- Data and logs are used in research to understand and improve the Lioness Device and Lioness Service; to troubleshoot the Lioness Service; to detect and protect against error, fraud or other criminal activity; and to enforce the Lioness Terms of Service.
- Aggregate data that does not identify you may be used to inform the health community about trends; for marketing and promotional use (for example, data may be included in an aggregated and anonymized chart that represents what a user can expect to see in the Lioness app); or for sale to interested audiences. (See "Aggregate Data – Non-Identifying Information" to learn more.)

WHAT KINDS OF DATA WE SHARE

Data That Could Identify You
Personally Identifiable Information (PII) is data that includes a personal identifier like your name,
email or address, or data that could reasonably be linked back to you. We will only share this data under the following circumstances:

- With companies that are contractually engaged in providing Lioness with services, such as order fulfillment, email management and credit card processing. These companies are obligated by contract to safeguard any PII they receive from us.
- If we believe that disclosure is reasonably necessary to comply with a law, regulation, valid legal process (e.g., subpoenas or warrants served on us), or governmental or regulatory request, to enforce or apply the Terms of Service or Terms of Sale, to protect the security or integrity of the Lioness Service, and/or to protect the rights, property, or safety of Lioness, its employees, users, or others. If we are going to release your data, we will do our best to provide you with notice in advance by email, unless we are prohibited by law from doing so.
- We may disclose or transfer your PII in connection with the sale, merger, bankruptcy, sale of assets or reorganization of our company. We will notify you if a different company will receive your PII and the promises in this Privacy Policy will apply to your data as transferred to the new entity.

Aggregate Data (Non-Identifying Data)
Lioness may share or sell aggregated data that does not identify you, with partners and the public in a variety of ways, such as by providing research or reports about health and sexuality. When we provide this information, we perform appropriate procedures so that the data does not identify you and we contractually prohibit recipients of the data from re-attributing it back to you.

Data That You Direct Us to Share
You can direct us to share data with other parties. For example, you might authorize us to link your Lioness account with a third-party app (e.g. a period tracking app) or send status updates to your Facebook or Twitter account (an example of this may be a tweet that you explicitly authorize us to send during a promotion or sweepstakes). Once you direct us to share your data with a third party, that data is governed by the third-party's privacy policy. You can revoke your consent for us to share data with the third party at any time.

WAYS YOU MIGHT SHARE YOUR DATA

Community Posts
The Lioness Service may offer discussion forums, message boards, social networking opportunities, chat pages and other public forums or features in which you may provide personal information, materials and related content. If you submit personal information when using these public features, please note that such personal information may be publicly posted and otherwise
disclosed and used without limitation or restriction.

Contests and Giveaways
Lioness may offer opportunities to participate in contests, giveaways and other promotions. Any data you submit in connection with these activities will be treated in accordance with this Privacy Policy, unless the rules for those offers note otherwise.

Surveys
Lioness may also ask you to participate in surveys (processed by Lioness or third parties) that help us understand consumer use of the Lioness Service. Any PII you provide to Lioness (or supplied by you or Lioness to such third-party survey providers) in connection with these surveys will only be used in relation to that survey and as stated in this policy.

THIRD PARTIES

Lioness will not be responsible for the practices of third parties that Lioness does not own or control or individuals that Lioness does not employ or manage. The information provided by you to other third parties may be subject to their own privacy policies, which may differ from Lioness's privacy policy.

The Lioness Service may contain links to other sites, and we make every effort to only link to sites that share our high standards and respect for privacy. However, we are not responsible for the privacy practices employed by other sites. Lioness is also not responsible for privacy or security issues with other Internet websites, even if a user of the Lioness Service posts the external link to the Lioness Service.

DATA RETENTION

Lioness reserves the right to retain your PII for as long as your account remains active. All information data is retained to comply with this policy or legal obligations. Lioness may continue to use your non-identifying data after you deactivate your account.

LIONESS’S POLICIES FOR MINORS

Lioness is not directed at persons under the age of 18. We do not knowingly collect any PII from minors under 18. If you are aware of a user under the age of 18 using Lioness, please contact us at help@lioness.io.

CAN I OPT-OUT OF RECEIVING LIONESS EMAILS?

Lioness may periodically contact you by sending an email newsletter, marketing emails and
emails related to new features. You will be able to opt-out of receiving these emails. If you opt out, we may still send you emails related to your account information and related to our business with you. Opting-out of these emails will not end transmission of important service-related emails that are necessary to your use of the Lioness Service.

HOW DOES LIONESS KEEP MY DATA SAFE?

Lioness uses a combination of technical and administrative security controls to maintain the security of your data. If you have a security-related concern, please contact Customer Support.

CONTACT US

PLEASE CONTACT US IF YOU HAVE ANY QUESTIONS ABOUT THIS POLICY.

Lioness
2001 Addison Street, Suite 300
Berkeley, CA 94704
203-805-8790
Help@lioness.io
The 'Spying Vibrator' Suit Is Over, But Sex Toys Are Still Talking Data

A few months back, the makers of We-Vibe smart sex toys found themselves facing litigation over the use of potentially intimate customer data. Last week, the company settled things for an amount that's TBD, but the matter of data collection-by-sex toy is far from put to bed.

Standard Innovation, the company behind We-Vibe couples' vibrators, is prepping a settlement agreement in response to a class action lawsuit brought by users, Ars Technica reports. The group, which included a plaintiff identified as “NP,” alleged that the company’s connected toys and mobile app collected real-time data on devices’ vibration settings, temperature, and duration of use without notifying customers. A pair of researchers separately suggested, too, that a security flaw in We-Vibe’s systems could
potentially be exploited by hackers (albeit from a close distance) to gain remote control over the wireless vibrators.

By early October, We-Vibe had tuned up security and detailed its new privacy policy for users, including easier steps for opting out of data collection. Among other things, the company told customers that they can use their vibrators without the app, or through the app but with data-sharing turned off, for a totally private experience.

A few days later, the Canadian company celebrated some of its latest tech-for-two with “Make Sex Exciting Again,” a multisensory event at New York’s Museum of Sex. Between showing excited visitors to the vibrator case craft table, aphrodesiac cocktail station, and decked-out Shaggin’ Wagon (with advice from Sex Nerd Sandra inside), We-Vibe’s Marketing Communication Manager Denny Alexander weighed in on the company’s since-averted drama over data.

He pointed out that, while the company remains committed to customers’ privacy, a certain amount of (anonymized) user data is necessary for any app to function. According to Alexander, real-world feedback from connected devices is particularly useful for sex-toy developers, too, given their decidedly discreet industry. “It’s a private, insular world, [mostly] without the benefit of consumer insights,” he said.

Because of We-Vibe’s very intimate (if important) aims, the company’s long quest toward the perfect design has principally relied on input and ideas from experts. Since the team was working to fill an uncharted niche, they also teamed up with researchers at Winkle to develop a new set of consumer criteria for questionnaires that would accurately gage the toys’ psychosocial and cultural reception. “We had to consider,
what does that even mean for us, as a company, to be asking about sex and intimacy,” Alexander said.

See also: Behold: The First Sex Toy On Kickstarter Is For Women, By Women

Only after a product has cleared these development stages, he said, does customer data come into play. Once it’s processed by a third party, We-Vibe uses the anonymized, aggregated info “only to validate and reaffirm” what feedback from testers and experts has told them. Alexander commented, “It gives us a general sense of users’ [vibration] intensity levels, steadiness of mode, and whether we’re marketing to the right people.”

Of course, when it comes to customers’ potentially intimate experiences, We-Vibe’s devices aren’t the only ones paying attention.

Aside from the usual fitness trackers, a number of fertility monitors now gather health data over time for patients to access, or share with their doctors, using a mobile app. Fertility and period-tracking apps, which report hormone levels based on simple responses to vital signs, have also been gaining momentum with women as tools for managing their reproductive, sexual, and overall health (and fret not, men: there’s now a fertility app for you, too).

In the sex-toy arena, numerous companies stand to get even more up close and personal with users than We-Vibe does, depending on design and on-board technology, while some are doing it right out in the open.

(Image courtesy Lioness via Indiegogo)
The team behind Lioness vibrators, for one, is using sophisticated bio-feedback from the devices to help map unique pleasure for women around the world. Sensors placed throughout the toy collect real-time data on a user’s temperature, muscle responses, and other physiological clues, while the Lioness app offers long-term insights on how, when, and under what circumstances women are maximizing their joy.

According to Lioness CEO and co-founder Liz Klinger, (safely) sharing this kind of information can be valuable in several ways. On Lioness’ end, such feedback contributes to a growing bank of expert testimony on how women find pleasure: a one-of-a-kind resource for helping each woman discover her own, Klinger says.

For users, data-based insights on their body’s ‘best practices’ can help spark conversations—and perhaps better connections—with their partners. She told Berkeley News, “[It’s] another way to frame the conversation … As like, this is how my body works … we can have this more objective conversation about just what do we like, how does the body work for you and me, and how can we work together on this?”

See also: A Powerful App Is Helping Survivors Fight Sexual Assault On Campuses Everywhere

ORing, on the other hand, has men’s health in mind when it comes to keeping score. Oivita, the company behind the wearable sex toy, explained by email that it lets men factor exercise and calories burned from “intimate activities” into their fitness planning.

The vibrating ring contains motion and gyro sensors for tracking calories burned as well as the “velocity, power strength, [and] movement counts” of loving sessions, according to the company. By syncing their ORings and Apple HealthKit accounts, users can also integrate this data into their overall wellness plan and records, while connecting with Apple Watch allows men to track their pulse, as well as their ongoing heart health, during sex.

Women aren’t left out of the the company’s sextech vision, either. The Oivita app offers to predict women’s sexual preferences and
moments of climax with its “Sex Coach” feature, from hip angle to strength—a sign of things to come, perhaps, with the company’s rumored ‘learning vibrator.’

Regardless of function, however, ‘connected’ technology always carries a privacy risk. The team behind the uber-popular game Pokemon Go, for example, recently closed a privacy hole in its programming that was netting massive amounts of user data. In 2015, researchers uncovered 256 iOS apps that were collecting users’ personal information—something Apple should have noticed and dealt with sooner, the researchers said.

For its part, Oivita offers users “full discretion” over how their data gets used, from its interaction with other applications to its accessibility. The company also assures customers that, given permission, it won’t use data for any other purposes than its stated performance goals.

See also: [The Entire Internet Is Being Archived In Canada For Safekeeping](#)

Klinger commented that thoughtful data-management is vital not only to Lioness’ customers, but to the company’s success. And when something is precious, of course, you want to keep it safe.

“For us, the information is the product and the only information that matters is that which benefits our users [so] we only collect information that can benefit our users and have extremely high standards for security and what we choose to collect,” she explained by email. “We’re also completely transparent about what we collect, and have an internal standard: if the users sat down and looked at what we collected,
would they not only grudgingly consent but enthusiastically agree with wanting us to have the data and provide our service from it.”

“Even though there are no industry standards yet, it’s something we take seriously because of the nature of what we do,” she added. “Any industry that develops connected devices needs to start thinking about that more.”

RECOMMENDED BY FORBES

In San Francisco, $8,000 Rent Includes Champagne Service By Robots

In Other News, This Cruelty-Free Lube Is Good For You (And Tastes Great!)

Sick Of Shallow Dating Apps? Sapio Breaks The Mold To Get Real

This VR Platform Invites Users To Have Virtual Sex With Real Performers

The 10 Most Dangerous U.S. Cities

Exclusive Interview: Oracle's Dave Donatelli On Company’s Cloud Strategy

The Toughest Jobs To Fill In 2017

Stan Lee Introduces Augmented Reality For His Kids Universe
23andMe escapes California class action for arbitration

By Erica Teichert | August 24, 2016

A federal appeals court ruled Tuesday that genetic testing company 23andMe can't be sued over allegations that it misled customers about its test kit because the claims belong in arbitration.

A unanimous panel at the 9th U.S. Circuit Court of Appeals in San Francisco affirmed a lower court's decision the class-action claims belonged in arbitration thanks to 23andMe's terms of service agreement. The plaintiffs sued back in 2013 alleging the Silicon Valley startup lied about its DNA test kit's health benefits, breached its warranty and used unfair business practices.

Until 2013, 23andMe claimed its saliva-based DNA testing kits could help customers prevent or mitigate diseases including diabetes, heart disease and breast cancer. But in November 2013, the Food and Drug Administration told the company to stop making such claims without agency approval. The Mountain View, Calif.-based company stopped selling the tests in December 2013 pending regulatory review before starting up again in October 2015.

In order to use the tests, customers had to agree to 23andMe's terms of service, which included an arbitration provision. Although the customers claimed various portions of the arbitration terms were unconscionable, the 9th Circuit rejected their arguments and deemed the agreement valid and enforceable.

23andMe offers 35 direct-to-consumer genetic tests that can tell users if they carry...
genetic mutations for diseases, including cystic fibrosis. It's a far cry from the more than 250 risk reports the company originally offered to customers.

RELATED CONTENT

23andMe faces class-action lawsuit in California
(http://www.modernhealthcare.com/article/20131203/INFO/312039984)
23andMe returns with FDA-approved genetic health tests
(http://www.modernhealthcare.com/article/20151021/news/151029975)
23andMe to follow FDA order to halt sales
(http://www.modernhealthcare.com/article/20131206/INFO/312069983)

Erica Teichert

Erica Teichert assigns, edits and directs news coverage for Modern Healthcare's website and magazine. She previously served as the publication’s New York bureau chief and legal reporter. Before joining Modern Healthcare in 2016, she worked at Law360 as legal newswire’s first D.C. bureau chief after three years as a court reporter covering the U.S. Supreme Court, D.C. Circuit and other federal courts and agencies. Prior to that, she worked as an associate editor for FierceMarkets. She has a bachelor's degree in communications with a print journalism emphasis from Brigham Young University.

Tags: Cancer, Diabetes, Genetic testing, Healthcare Information Technology, Technology
October 27, 2016

Tompkins v. 23andME, Inc.

Headline: Ninth Circuit panel holds pursuant to the Federal Arbitration Act, 9 U.S.C. § 2 (“FAA”) and California’s unconscionability rules that provisions in a mandatory arbitration clause in an online consumer contract of adhesion are valid and enforceable.


Issues Presented: (1) Whether provisions in an online mandatory arbitration clause authorizing an award of attorney fees and costs to the prevailing party, designating the forum for arbitrations, and excluding intellectual property disputes from arbitration are unconscionable. (2) Whether other provisions of the online agreement establishing a one-year statute of limitations and giving 23andMe a unilateral right to modify the contract render the arbitration provision unconscionable.

Brief Summary: Plaintiffs are customers of 23andMe, Inc., who purchased DNA test kits on-line. They filed a class action lawsuit claiming that provisions of their agreement with 23andMe relating to mandatory arbitration are unconscionable. (2) Whether other provisions of the online agreement establishing a one-year statute of limitations and giving 23andMe a unilateral right to modify the contract render the arbitration provision unconscionable. For arbitration proceedings; and exempting from mandatory arbitration any disputes relating to intellectual property rights, obligations, or any infringement claims. Plaintiffs also claimed that other contract provisions establishing a one-year statute of limitations period and giving 23andMe a unilateral right to modify the agreement rendered the arbitration clause unconscionable. 23andMe responded with a motion to compel arbitration. The district court granted 23andMe’s motion and plaintiffs appealed.

The Ninth Circuit panel recognized that the Federal Arbitration Act, 9 U.S.C. § 2, establishes a strong national policy favoring arbitration. A court may invalidate an arbitration agreement under the "savings clause" of § 2 only in cases where generally applicable contract defenses such as fraud, duress, or unconscionability are present. The court then examined California law to determine whether the provisions would be held unconscionable under that state’s law.

The Ninth Circuit concluded that the provision awarding attorney fees and costs to the prevailing party is not unconscionable under California law. Although California appellate courts have held unilateral cost shifting clauses in the arbitration context to be unconscionable, the plaintiffs failed to show the unconscionability doctrine's application in bilateral provision cases. The court also rejected plaintiffs' claim that the fees and costs to the losing party would be too great for plaintiffs to bear as they failed to provide evidence on this point. Second, the Court held that plaintiffs did not prove that the cost and inconvenience of having arbitrations in San Francisco was unreasonable. Third, plaintiffs failed to identify or raise any intellectual property claims that 23andMe might bring against them.

The court next addressed the contract provisions creating the one-year statute of limitations and giving 23andMe the unilateral right to modify the contract. The Ninth Circuit noted that, as a general rule, where the arbitration agreement itself is not unconscionable, provisions outside the arbitration agreement will not make it so. The court relied on California case precedents in finding the one-year statute of limitations was not unconscionable. It also held that plaintiffs could challenge the enforceability of the modification clause in the arbitration proceeding.

Significance: Consumer contracts formed online between individuals and corporations often include mandatory arbitration clauses. The Federal Arbitration Act established a strong national policy favoring arbitration. Federal courts will enforce a mandatory arbitration clause unless an aggrieved party can prove the provision is procedurally and substantively unconscionable under relevant state law.

Extended Summary: 23andMe sold DNA testing kits to customers online through its website. It claimed its service could assist customers in managing health risks as well as preventing or mitigating certain diseases. Before a customer could purchase the kit, the individual was required to click on a link to the company’s terms of service and check a box that acknowledged the buyer’s assent to the terms. The agreement included a mandatory arbitration provision. The provision authorized an award of fees and costs to the prevailing party and required that arbitration proceedings be governed by California law and held in San Francisco, California. The arbitration clause specifically excluded from arbitration "disputes relating to intellectual property rights, obligations, or any infringement claims.” Other contract provisions established a one-year statute of limitations and gave 23andMe a unilateral right to modify the agreement.

In November 2013, the Food and Drug Administration ordered 23andMe to discontinue marketing its services for health purposes until it obtained government approval. Plaintiffs are customers who had purchased DNA test kits online. They brought a number of class action suits against 23andMe, alleging unfair business practices, breach of warranty, and misrepresentation. By agreement, all claims were consolidated in the United States District Court for the Northern District of California.

23andMe filed a motion to compel all plaintiffs to arbitrate their claims. Plaintiffs responded that the mandatory arbitration provision and other clauses of the agreement were unconscionable. The district court found for 23andMe and granted its motion to compel arbitration. Plaintiffs filed a timely appeal.

The Ninth Circuit affirmed the district court decision. The court began its opinion by recognizing that § 2 of the FAA “is a congressional declaration of a liberal federal policy favoring arbitration agreements.” Any doubts about the scope of arbitrable issues, including applicable contract defenses, are to be resolved in favor of arbitration. Moses H Cone Memorial Hospital v. Mercury Construction Co., 460 U.S. 1, 24-25 (1983). The court noted that the "savings clause" of § 2
authorizes a court to strike or limit an arbitration provision only in instances involving generally applicable contract defenses, such as fraud, duress, or unconscionability. It held that a federal court must look to relevant state law in deciding whether an arbitration provision is unconscionable. For this reason, the Ninth Circuit examined California authorities to decide whether provisions of the arbitration clause in the instant case were unconscionable.

Under California law, the doctrine of unconscionability is applicable if the written contract is both procedurally and substantively unconscionable, though they need not be present to the same degree. Procedural unconscionability focuses on oppression or surprise due to unequal bargaining power while substantive unconscionability relates to overly harsh or one-sided results. Sanchez v. Valencia Holding Co., 61 Cal. 4th 899, 910 (2015).

The Ninth Circuit first examined the provision in the arbitration clause stating “arbitration costs and reasonable documented attorneys’ costs of both parties will be borne by the party that ultimately loses.” Plaintiffs contended that if they lost, the arbitrators’ charge of $1,500 per day and 23andMe’s “top tier” lawyers’ fees would be unreasonable, overly burdensome, and unfair. The Ninth Circuit panel reviewed relevant California authorities and found that a number of courts had enforced prevailing party clauses in the non-arbitration context. In cases involving arbitration, several California appellate courts held cost shifting clauses unconscionable where they were unilateral, thus available to only one side. But plaintiffs were unable to produce any case where a bilateral clause awarding attorney fees and costs to the prevailing party was unconscionable. Indeed, Cal. Civil Code § 1717 appears to approve bilateral prevailing party clauses. For these reasons, the Ninth Circuit concluded that the bilateral prevailing party clause in this case was not unconscionable. The court also held that plaintiffs did not offer evidence to show that the arbitration costs and attorney fees would be unaffordable or thwart their ability to arbitrate the dispute.

Next, the Ninth Circuit addressed plaintiffs’ claim that the designation of San Francisco as the forum for arbitration was unconscionable. It discussed the California Supreme Court's decision in Valenti & Smith, Inc. v. Superior Court, 17 Cal. 3d 491 (1976), which rejected plaintiff's claim that a venue clause was unenforceable because of inconvenience and expense of the forum. In the absence of a showing that such a clause is unreasonable, a forum selection clause is generally valid and enforceable. Further case analysis indicates that the plaintiff has a heavy burden of proof to show a forum-selection clause is unconscionable. This is so even if the clause appears in an adhesion contract. Mere inconvenience or additional expense is not the test. So long as the party had adequate notice as to the forum’s location, the clause is enforceable. Here, the Ninth Circuit panel concluded that San Francisco was not an unreasonable choice. San Francisco has a proper connection to the contract as it is 23andMe’s principal place of business, seven of the plaintiffs reside in California, and six of the nine actions were filed in California. In addition, the two affidavits claiming financial hardship did not explain why the expense of travelling to the San Francisco venue would be burdensome.

The final arbitration clause provision discussed by the Ninth Circuit exempted "any disputes relating to intellectual property rights, obligations, or any infringement claims" from mandatory arbitration. The court cited California authority stating that substituting arbitration for litigation resulted in no inherent disadvantage. Sonic-Calabasas A, Inc. v. Moreno, 57 Cal. 4th 1109, 1152 (2013). Moreover, a one-sided contract is not necessarily unconscionable. The Ninth Circuit also found that the plaintiffs did not identify any intellectual property right that 23andMe was likely to bring against its customers. The rights that were included in arbitration are ones that the plaintiffs are likely to sue on and there was therefore a bilateral aspect to the clause. 23andMe demonstrated the need for the clause since it provided its business with a "margin of safety," which in itself, was not unconscionable. For these reasons, the court held the arbitration clause was enforceable.

The plaintiffs also challenged contract terms creating the one-year statute of limitations and the unilateral right of 23andMe to modify the agreement. The plaintiffs contended that these two provisions rendered the arbitration clause unconscionable. The Ninth Circuit reviewed these issues and ruled that both were enforceable. The court cited Rent-A-Center, W, Inc. v. Jackson, 561 U.S. 63, 70-71 (2010), where the Supreme Court held that a party's challenge to a contract provision or to the contract as a whole does not prevent a court from enforcing an agreement to arbitrate. It cited California authority showing that it was not unconscionable for parties in contractual relations do modify a statute of limitations. The one-year statute of limitations in this case was bilateral; it applied to both parties and both parties had adequate notice and agreed to the provision. As for the provision granting 23andMe the unilateral right to modify the contract, even if this clause is unconscionable, it would not make the arbitration provision or the contract as a whole unenforceable. The Ninth Circuit decided that the plaintiffs are free to argue during arbitration that the unilateral modification clause itself is unenforceable and did not reach that claim in the appeal.

For these reasons, the Ninth Circuit affirmed the district court's decision to grant the motion to compel arbitration.

To read the full opinion, please visit: https://cdn.ca9.uscourts.gov/datastore/opinions/2016/08/23/14-16405.pdf


Argument Date: May 12, 2016

Date of Issued Opinion: August 23, 2016

Docket Number: 14-16405

Decided: Affirmed.

Case Alert Author: David Griego

Counsel: Jeremy Robinson (argued), Jason C. Evans, and Gayle M. Blatt; Casey, Gerry, Schenk, Francavilla, Blatt &Penfield, LLP, San Diego, California; Mark Ankorn, Ankorn Law Firm, PC, San Diego, California; for Plaintiff-Appellant
ORDER

The opinion filed August 23, 2016, is hereby amended as follows:

On page 1031 of the opinion:

< Given this precedent, our authority to review portions of the contract outside the arbitration provision is limited, if it exists at all. Even assuming we can review the two outside provisions, we are limited to considering whether, in the specific circumstances of the parties and the context in which the contract was formed, these outside provisions contribute to making the arbitration provision itself unconscionable. > is amended to:

< Given this precedent, our authority to review portions of the contract outside the arbitration provision is limited. But as Rent-A-Center indicates, "[i]t may be that" where a plaintiff challenges "the validity under § 2 of the precise agreement to arbitrate at issue" on the ground that certain general contract provisions "as applied" to the agreement to arbitrate render it unconscionable, such a "challenge should [be] considered by the court." 561 U.S. at 71, 74 [130 S.Ct. 2772] (emphasis in original). >.

On page 1031 of the opinion, the following sentence is deleted:

< As a general rule where the arbitration agreement itself is not unconscionable, provisions outside the arbitration agreement will not make it so. >.

On page 1031-32 of the opinion:

< Likewise, the unilateral modification clause does not make the arbitration provision itself unconscionable. >
is amended to:

< Likewise, under the circumstances here, the unilateral modification clause does not make the arbitration provision itself unconscionable. >.

No further petitions for rehearing or rehearing en bane will be entertained from this amendment.

**OPINION**

IKUTA, Circuit Judge:

Under the terms of the agreement at issue here, the customers of 23andMe, Inc., were required to arbitrate the present action. The district court enforced the terms of that agreement and granted 23andMe's motion to compel arbitration. We hold that none of the challenged portions of the arbitration provision, alone or in concert, render the arbitration provision unconscionable under current California law. We therefore affirm.

23andMe, Inc., provides a direct-to-consumer genetic testing service, which it calls the "Personal Genome Service." A customer interested in obtaining the genetic testing service must visit the 23andMe website to purchase an online DNA testing kit. When purchasing the kit, the customer can click on a link to the company's Terms of Service that was available at the bottom of the webpage. However, the customer is not required to read or click through the terms before making a purchase.

After receiving the kit, the customer returns to the website to create an online account with 23andMe to register the DNA kit. At this stage, and in order to proceed to use the genetic testing service, a customer has to click on a box indicating agreement to the Terms of Service. The Terms of Service is a multipage agreement which states that it constitutes the entire agreement between 23andMe and its customers. Paragraph 28(b) of the Terms of Service contains a mandatory arbitration provision which states, in full:

> **1021 Applicable law and arbitration. Except for disputes relating to intellectual property rights, obligations, or any infringement claims, any disputes with 23andMe arising out of or relating to the Agreement ("Disputes") shall be governed by California law regardless of your country of origin or where you access 23and-Me, and notwithstanding of any conflicts of law principles and the United Nations Convention for the International Sale of Goods. Any Disputes shall be resolved by final and binding arbitration under the rules and auspices of the American Arbitration Association, to be held in San Francisco, California, in English, with a written decision stating legal reasoning issued by the arbitrator(s) at either party's request, and with arbitration costs and reasonable documented attorneys' costs of both parties to be borne by the party that ultimately loses. Either party may obtain injunctive relief (preliminary or permanent) and orders to compel arbitration or enforce arbitral awards in any court of competent jurisdiction.**

After conducting a self-test, a customer would send the completed DNA kit to 23andMe, which performed the genetic testing services and provided the results to the customer.

Until 2013, 23andMe claimed that its service could be used to help customers manage health risks, as well as prevent or mitigate diseases such as diabetes, heart disease, and breast cancer. In November 2013, the Food and Drug Administration (FDA) told 23andMe to discontinue marketing its services for health purposes until the company obtained government approval. The company then ceased its health-related marketing.

As a result of the FDA's determination, multiple plaintiffs filed different class actions against 23andMe relating to the company's health claims. The claims were consolidated by agreement in federal district court in the Northern District of California. David Tompkins represents a consolidated class of customers bringing a number of separate causes of actions against 23andMe for unfair business practices, breach of warranty, and misrepresentations about the health benefits of 23And-Me's services. All the named plaintiffs in the present action purchased a DNA test kit, created an online account with 23and-Me to register their DNA kits, and assented to the Terms of Service.

In April 2014, 23andMe filed a motion to compel all plaintiffs to arbitrate their claims. A few months later, the district court granted 23andMe's motion. After reviewing the mandatory arbitration provision in the Terms of Service, the district court concluded that
although the arbitration provision was procedurally unconscionable, it was not substantively unconscionable and therefore was enforceable under California law. The court held that plaintiffs' other challenges to the Terms of Service had to be determined by the arbitrator in the first instance. Plaintiffs timely appealed.

The district court had jurisdiction under 28 U.S.C. § 1332(d)(2) because the parties satisfied minimal diversity and the amount in controversy exceeded $5 million. We have jurisdiction under 28 U.S.C. § 1291 and 9 U.S.C. § 16(a)(3). We "review de novo district court decisions about the arbitrability of claims." Kramer v. Toyota Motor Corp., 705 F.3d 1122, 1126 (9th Cir. 2013). We review factual findings for clear error. Balen v. Holland Am. Line Inc., 583 F.3d 647, 652 (9th Cir. 2009), and review "[t]he interpretation and meaning of contract provisions" de novo. Lee v. Intelius Inc., 737 F.3d 1254, 1258 (9th Cir. 2013).

In order to determine whether a state legislative or common law rule makes an agreement to arbitrate unenforceable, we must consider both the federal law of arbitration and the state rule at issue.

A

Congress enacted the Federal Arbitration Act (FAA) in 1925 in order to "counter prevalent judicial refusal to enforce arbitration agreements." Mortensen v. Bresnan Comm'ns, 722 F.3d 1151, 1157 (9th Cir. 2013). Section 2 of the FAA makes a written provision in a contract to settle a controversy by arbitration "valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract." 9 U.S.C. § 2. Section 2 is a congressional declaration of a liberal federal policy favoring arbitration agreements. Moses H. Cone Mem'l Hosp. v. Mercury Constr. Corp., 460 U.S. 1, 24, 103 S.Ct. 927, 74 L.Ed.2d 765 (1983). "The overarching purpose of the FAA ... is to ensure the enforcement of arbitration agreements according to their terms so as to facilitate streamlined proceedings." AT & T Mobility LLC v. Concepcion, 563 U.S. 333, 344, 131 S.Ct. 1740, 179 L.Ed.2d 742 (2011). Any doubts about the scope of arbitrable issues, including applicable contract defenses, are to be resolved in favor of arbitration. Moses H Cone, 460 U.S. at 24-25, 103 S.Ct. 927; Ferguson v. Corinthian Colls., Inc., 733 F.3d 928, 938 (9th Cir. 2013).

The Supreme Court has long made clear that the FAA's "national policy favoring arbitration" also applies to the states. See, e.g., Southland Corp. v. Keating, 465 U.S. 1, 10, 104 S.Ct. 852, 79 L.Ed.2d 1 (1984). The FAA forecloses both "state legislative attempts to undercut the enforceability of arbitration agreements," id., at 16, 104 S.Ct. 852, and state common law principles that interfere with "the enforcement of arbitration agreements according to their terms." Concepcion, 563 U.S. at 344, 131 S.Ct. 1740. The text of the FAA makes only one exception to the validity of an arbitration agreement: the savings clause in § 2 provides that a court may strike or limit an arbitration provision on "such grounds as exist at law or in equity for the revocation of any contract." 9 U.S.C. § 2. The savings clause "permits agreements to arbitrate to be invalidated by generally applicable contract defenses, such as fraud, duress, or unconscionability," but not by defenses that apply only to arbitration or that derive their meaning from the fact that an agreement to arbitrate is at issue. Concepcion, 563 U.S. at 339, 131 S.Ct. 1740 (quoting Doctor's Assocs., Inc. v. Casarotto, 517 U.S. 681, 687, 116 S.Ct. 1652, 134 L.Ed.2d 902 (1996)). "[I]n assessing the rights of litigants to enforce an arbitration agreement" a court may not "construe that agreement in a manner different from that in which it otherwise construes nonarbitration agreements under state law." Perry v. Thomas, 482 U.S. 483, 492 n.9, 107 S.Ct. 2520, 96 L.Ed.2d 426 (1987).

Even when the state rule at issue is "a doctrine normally thought to be generally applicable," such as unconscionability, it may nevertheless be preempted if it has "1023 been "applied in a fashion that disfavors arbitration," Concepcion, 563 U.S. at 341, 131 S.Ct. 1740, or in a manner that, in practice, would "have a disproportionate impact on arbitration agreements," id. at 342, 131 S.Ct. 1740. We have interpreted this rule broadly, holding that "[a]ny general state-law contract defense, based in unconscionability or otherwise, that has a disproportionate effect on arbitration is displaced by the FAA." Mortensen, 722 F.3d at 1159.

The plaintiffs here challenge the 23andMe arbitration provision under the California doctrine of unconscionability. Under the savings clause in § 2, we must first determine whether California has a generally applicable unconscionability doctrine that would make the arbitration provision invalid. In discerning California law, "[d]ecisions of the California Supreme Court, including reasoned dicta, are binding on us as to California law." Muniz v. United Parcel Serv., Inc., 738 F.3d 214, 219 (9th Cir. 2013). "When the state's highest court has not squarely addressed an issue, we must predict how the highest state court would decide the issue using intermediate appellate court decisions, decisions from other jurisdictions, statutes, treaties and restatements for guidance." Glendale Assoc's., Ltd. v. NLRB, 347 F.3d 1145, 1154 (9th Cir. 2003) (internal quotation marks omitted). "Decisions of the six district appellate courts
are persuasive but do not bind each other or us," although we generally will "follow a published intermediate state court decision regarding California law unless we are convinced that the California Supreme Court would reject it." *Muniz*, 738 F.3d at 219.

**B**

Under California law, a state court may refuse to enforce a provision of a contract if it finds that the provision was "unconscionable at the time it was made." Cal. Civil Code § 1670.5(a). Courts may find a contract as a whole "or any clause of the contract" to be unconscionable. *Id.* The party asserting that a contractual provision is unconscionable bears the burden of proof. *Sanchez v. Valencia Holding Co., LLC*, 61 Cal.4th 899, 911, 190 Cal.Rptr.3d 812, 353 P.3d 741 (2015). Unconscionability has "both a procedural and a substantive element, the former focusing on oppression or surprise due to unequal bargaining power, the latter on overly harsh or one-sided results." *Id.* at 910, 190 Cal.Rptr.3d 812, 353 P.3d 741 (internal quotation marks omitted). Both procedural and substantive unconscionability must be present in order for a clause to be unconscionable, but they need not necessarily be present to the same degree. *Armedariz v. Found. Health Psychcare Services*, 24 Cal.4th 83, 114, 99 Cal.Rptr.2d 745, 6 P.3d 669 (2000). Although California courts have characterized "substantive unconscionability" in various ways, "[a]ll of these formulations point to the central idea that unconscionability doctrine is concerned not with 'a simple old-fashioned bad bargain' but with terms that are 'unreasonably favorable to the more powerful party.'" *Sonic-Calabasas A, Inc. v. Moreno*, 57 Cal.4th 1109, 1145, 163 Cal.Rptr.3d 269, 311 P.3d 184 (2013) (Sonic II).

Under California law, "[a]n evaluation of unconscionability is highly dependent on context." *Sanchez*, 61 Cal.4th at 911, 190 Cal.Rptr.3d 812, 353 P.3d 741. California courts give the parties "a reasonable opportunity to present evidence as to [the provision's] commercial setting, purpose, and effect," Cal. Civil Code § 1670.5, and then examine the context in which the contract was formed and the "respective circumstances of the parties" as they existed at the formation of the agreement. *Nagrampa v. Mailcoup, Inc.*, 57 Cal.4th 1109, 1145, 163 Cal.Rptr.3d 269, 311 P.3d 184 (2013) (quoting *Bolter v. Super. Ct.*, 87 Cal.App.4th 900, 909, 104 Cal.Rptr.2d 888 (Cal. Ct. App. 2001)).

The California Supreme Court has recently revisited the general principles of unconscionability under state law, and has explained how they apply to arbitration provisions in light of *Concepcion* and other recent U.S. Supreme Court cases. See *Baltazar v. Forever 21, Inc.*, 62 Cal.4th 1237, 200 Cal. Rptr.3d 7, 367 P.3d 6 (2016); *Sanchez*, 61 Cal.4th at 911, 190 Cal.Rptr.3d 812, 353 P.3d 741; *Sonic II*, 57 Cal.4th at 1143-45, 163 Cal.Rptr.3d 269, 311 P.3d 184. In doing so, the California Supreme Court confirmed that California’s "unconscionability standard is, as it must be, the same for arbitration and nonarbitration agreements" under the FAA’s savings clause. *Sanchez*, 61 Cal.4th at 912, 190 Cal.Rptr.3d 812, 353 P.3d 741. We are bound by the California Supreme Court’s most recent articulation of its standard in determining whether the arbitration provisions challenged by plaintiffs are unconscionable. See, e.g., *In re NCAA Student-Athlete Name & Likeness Licensing Litig.*, 724 F.3d 1268, 1278 (9th Cir. 2013).

**III**

We now apply these principles to the plaintiffs’ claim that the arbitration provision in Paragraph 28(b) of the Terms of Service is substantively unconscionable. The plaintiffs challenge the provision’s prevailing party clause, the forum selection clause, and the clause excluding intellectual property claims from arbitration. They claim that these clauses together, along with the one-year statute of limitations and 23andMe’s right to modify the Terms of Service, render the provision unenforceable. We consider these claims in turn.

**A**

We first turn to the arbitration provision’s prevailing party clause, which states that "arbitration costs and reasonable documented attorneys’ costs of both parties” will "be borne by the party that ultimately loses." Plaintiffs claim that this provision is unconscionable because AAA arbitrators charge $1500 a day for arbitration, and 23andMe’s "top-tier lawyers" would also have significant charges. We begin with California cases addressing the enforceability of prevailing party clauses that shift attorneys’ fees to the losing party. The California Supreme Court has held that as a general rule, “[p]arties may validly agree that the prevailing party will be awarded attorney fees incurred in any litigation between themselves, whether such litigation sounds in tort or in contract.” *Santisas v. Goodin*, 17 Cal.4th 599, 608, 71 Cal.Rptr.2d 830, 951 P.2d 399 (1998) (quoting *Xuereb v. Marcus & Millichap, Inc.*, 3 Cal.App.4th 1338, 1341, 5 Cal.Rptr.2d 154 (1992)). A number of California appellate courts have enforced prevailing party clauses under this general
rule in the nonarbitration context. See *Lennar Homes of Cal., Inc. v. Stephens*, 232 Cal.App.4th 673, 694, 181 Cal. Rptr.3d 638 (Cal. Ct. App. 2014) ("[T]here is nothing generally absurd or unconscionable about prevailing party clauses."); *Maynard v. BTI Gro., Inc.*, 216 Cal. App. 4th 984, 989, 157 Cal.Rptr.3d 148 (Cal. Ct. App. 2013) ("It is clear from the case law ... that parties may validly agree that the prevailing party will be awarded attorney fees incurred in any litigation between themselves.").

Several state appellate courts have held that provisions shifting attorneys' fees are unconscionable in the arbitration context,* 1025 see, e.g., *Carmona v. Lincoln Millennium Car Wash, Inc.*, 226 Cal.App.4th 74, 88, 171 Cal.Rptr.3d 42 (Cal. Ct. App. 2014); *Samaniego v. Empire Today LLC*, 205 Cal.App.4th 1138, 1143, 140 Cal.Rptr.3d 492 (Cal. Ct. App. 2012); *Ajamian v. CantorCO2e, L.P.*, 203 Cal.App.4th 771, 799-800, 137 Cal.Rptr.3d 773 (Cal. Ct. App. 2012). These cases, however, all involved unilateral, rather than bilateral fee-shifting provisions. For instance, *Carmona* considered a provision in an arbitration agreement between a buyer and seller that permitted the seller to recover attorneys' fees and costs whenever it instituted litigation or arbitration, and did not give employees any reciprocal right. The court held that this clause contributed to unconscionability because it was "oppressively one-sided and unenforceable as written" under section 1717 of the California Civil Code. *Id.* at 89, 171 Cal.Rptr.3d 42. Similarly, Samaniego noted that a clause which required the employees to pay attorneys' fees incurred by the employer, but imposed no reciprocal obligation on the employer to pay the employees' fees, "contributes to a finding of unconscionability." *205 Cal.App.4th at 1147, 140 Cal.Rptr.3d 492; see also Ajamian, 203 Cal.App.4th at 799, 137 Cal. Rptr.3d 773* (invalidating a clause that required the employee, but not the employer, to pay both parties' attorneys' fees because "[t]he provision is obviously not mutually and, on that basis alone, is unconscionable and unenforceable.").

By contrast, the plaintiffs have not identified any case where a state appellate court held that a bilateral clause awarding attorneys' fees and costs to the prevailing party was unconscionable, whether in an arbitration or nonarbitration context. Indeed, section 1717 of the California Civil Code appears to approve such bilateral prevailing party clauses, since it requires courts to treat all unilateral prevailing party clauses as if they were bilateral clauses.* 1025 This rule is equally applicable to contracts of adhesion. See *Sys. Inv. Corp. v. Union Bank*, 21 Cal.App.3d 137, 163, 98 Cal.Rptr. 735 (Cal. Ct. App. 1971) ("Section 1717 was enacted to make all parties to a contract, especially an "adhesion contract," equally liable for attorney's fees and other necessary disbursements.").

In this case, the prevailing party clause is explicitly bilateral, providing that either party can request binding arbitration, and the "arbitration costs and reasonable documented attorneys' costs of both parties [are] to be borne by the party that ultimately loses," whoever that might be. In light of the California Supreme Court's ruling that the standard for unconscionability must be the same for "arbitration costs and reasonable documented attorneys' costs of both parties [are] to be borne by the party that ultimately loses," *Sanchez*, 61 Cal.4th at 911, 190 Cal.Rptr.3d 812, 353 P.3d 741, and the general rule that parties may validly agree to a bilateral prevailing party clause, see *Santisas*, 17 Cal.4th at 608, 71 Cal.Rptr.2d 830, 951 P.2d 399; *see also Cal. Civ. Code § 1717*, we conclude that the bilateral attorneys' fee shifting clause in the Terms of Service is not unconscionable under California law.

Plaintiffs next claim that the portion of the prevailing party clause that shifts the arbitrators' fees to the losing party is unconscionable because it would * 1026 require consumers to shoulder fees that they would not have to bear in litigation.

We again start with California Supreme Court precedent. Plaintiffs rely on *Armendariz v. Foundation Health Psychcare Services*, which held that "when an employer imposes mandatory arbitration as a condition of employment, the arbitration agreement or arbitration process cannot generally require the employee to bear any type of expense that the employee would not be required to bear if he or she were free to bring the action in court." *24 Cal.4th at 110-11, 99 Cal.Rptr.2d 745, 6 P.3d 669.* We have previously struck down arbitration fee-shifting clauses as unconscionable under this *Armendariz* rule. See, e.g., *Pokorny v. Quixtar, Inc.*, 601 F.3d 987, 1004 (9th Cir. 2010); *Ting v. AT & T*, 319 F.3d 1126, 1135 (9th Cir. 2003).

The California Supreme Court has since indicated that this *Armendariz* rule is limited to the employment context. See *Sanchez*, 61 Cal.4th at 918-19, 190 Cal.Rptr.3d 812, 353 P.3d 741. In the area of consumer arbitration, *Sanchez* explained, the California legislature took a different approach by enacting section 1284.3 of the California Code of Civil Procedure. *Id.* Section 1284.3 provides that "[a]ll fees and costs charged to or assessed upon a consumer party by a private arbitration company in a consumer arbitration, exclusive of arbitrator fees, shall be waived for an indigent consumer." Cal. Civ. Proc. § 1284.3(b)(1). According to *Sanchez*, this shows the legislature's decision to adopt "an ability-to-pay approach" to arbitration fees in the consumer context, requiring a "case-by-case determination of affordability" for consumers, and a rejection of the *Armendariz* categorical approach. *61 Cal.4th at 919, 190 Cal.Rptr.3d 812, 353 P.3d 741*. *Sanchez* explained that while "jobseekers are more likely to face 'particularly acute' economic pressure to sign an employment contract with a predispute arbitration provision ... [c]onsumers, who face significantly less economic pressure, would seem to require measurably less protection." *Id.* at 919-20, 190 Cal.Rptr.3d 812, 353 P.3d 741. Deferring to this legislative determination, *Sanchez* held that in the consumer context, a fee-shifting "provision cannot be
the California Supreme Court have placed a heavy burden on a plaintiff seeking to defeat such a clause, requiring it to demonstrate inconvenience and expense of the forum. 551 P.2d 1206. In particular, "freely and voluntarily by parties who have negotiated at arm's length," unreasonable if "the forum selected would be unavailable or unable to accomplish substantial justice." In Smith, Valentino & Smith, Inc. v. Superior Court, 17 Cal.3d 491, 495-96, 131 Cal.Rptr. 374, 551 P.2d 1206 (1976) (In Bank), exemplifies California's unconscionability doctrine with respect to forum selection clauses. See Sanche, 61 Cal.4th at 911, 190 Cal.Rptr.3d 812, 353 P.3d 741. We therefore conclude that the plaintiffs here did not carry their burden of demonstrating the substantive unconscionability of the bilateral prevailing party clause.

B

We next turn to the arbitration provision's forum selection clause, which states that final and binding arbitration proceedings will be held in San Francisco, California. Plaintiffs claim that the district court should have concluded this clause was substantively unconscionable because it could potentially require consumers to travel from a faraway city or state for a small potential recovery. Because those costs involved in traveling outweigh any potential remedies, plaintiffs argue, consumers are effectively forced to give up the right to pursue their claim. As evidence, plaintiffs point to affidavits by two of the nine plaintiffs stating that the cost of traveling to San Francisco for arbitration would be burdensome and expensive.

We begin by considering when a forum selection clause is unconscionable under California law. The California Supreme Court recently indicated that its decision in Smith, Valentino & Smith, Inc. v. Superior Court, 17 Cal.3d 491, 495-96, 131 Cal.Rptr. 374, 551 P.2d 1206 (1976) (In Bank), exemplifies California's unconscionability doctrine with respect to forum selection clauses. See Sanche, 61 Cal.4th at 911, 190 Cal.Rptr.3d 812, 353 P.3d 741 (citing Smith, Valentino, 17 Cal.3d at 495-96, 131 Cal.Rptr. 374, 551 P.2d 1206). Smith, Valentino joined the "modern trend which favors enforceability" of forum selection clauses, and concluded "that forum selection clauses are valid and may be given effect, in the court's discretion and in the absence of a showing that enforcement of such a clause would be unreasonable." 17 Cal.3d at 495-96, 131 Cal.Rptr. 374, 551 P.2d 1206. A clause would be unreasonable if "the forum selected would be unavailable or unable to accomplish substantial justice." Id. at 494, 131 Cal.Rptr. 374, 551 P.2d 1206. In particular, Smith, Valentino rejected the plaintiffs arguments that the clause was unconscionable because of the inconvenience and expense of the forum. Id. at 496, 131 Cal.Rptr. 374, 551 P.2d 1206. Because the contract had been "entered into freely and voluntarily by parties who have negotiated at arm's length," Smith, Valentino concluded that the parties "reasonably can be held to have contemplated in negotiating their agreement the additional expense and inconvenience attendant on the litigation of their respective claims in a distant forum," and therefore "mere inconvenience or additional expense is not the test of unreasonableness since it may be assumed that the plaintiff received under the contract consideration for these things." Id.

*1028 Following Smith, Valentino, California courts have generally expressed a policy approving forum selection clauses because they "play an important role in both national and international commerce," Lu v. Dryclean-U.S.A. of California, Inc., 11 Cal.App.4th 1490, 1493, 14 Cal.Rptr.2d 906 (Cal. Ct. App. 1992), and "provide a degree of certainty, both for business and their customers, that contractual disputes will be resolved in a particular forum," Net2Phone, Inc. v. Super. Ct., 109 Cal. App.4th 583, 588, 135 Cal.Rptr.2d 149 (Cal. Ct. App. 2003). "Given the importance of forum selection clauses, both the United States Supreme Court and the California Supreme Court have placed a heavy burden on a plaintiff seeking to defeat such a clause, requiring it to demonstrate that enforcement of the clause would be unreasonable under the circumstances of the case." Lu, 11 Cal.App.4th at 1493, 14 Cal.Rptr.2d 906.

Although Smith, Valentino approved a forum selection clause in a negotiated contract, California appellate courts have implemented this broader policy and enforced forum selection clauses in adhesion contracts in a non-arbitration context. In Intershop Communications v. Superior Court, the court agreed that an employment contract was a contract of adhesion, but nevertheless held
that its forum selection clause, requiring disputes to be litigated in Germany, was enforceable. 104 Cal. App.4th 191, 201, 127 Cal.Rptr.2d 847 (Cal. Ct. App. 2002). "A forum selection clause within an adhesion contract will be enforced as long as the clause provided adequate notice to the [party] that he was agreeing to the jurisdiction cited in the contract." Id. at 201-02, 127 Cal.Rptr.2d 847 (internal quotation marks omitted); see also Olinick v. BMG Entmt'l, 138 Cal. App.4th 1286, 1294, 42 Cal.Rptr.3d 268 (Cal. Ct. App. 2006) (upholding a forum selection clause in an employment contract, and stating that "mere inconvenience or additional expense is not the test of unreasonableness of a mandatory forum selection clause" (internal quotation marks omitted)). California appellate courts considering forum selection clauses in adhesion contracts have held that "[n]either inconvenience nor additional expense in litigating in the selected forum is part of the test of unreasonableness." Cal-State Bus. Prosds. & Servs., Inc. v. Ricoh, 12 Cal. App.4th 1666, 1679, 16 Cal.Rptr.2d 417 (Cal. Ct. App. 1993); see also Am. Online, Inc. v. Superior Court, 90 Cal.App.4th 1, 19, 108 Cal.Rptr.2d 699 (Cal. Ct. App. 2001) (rejecting the argument that a forum selection clause in an adhesion contract was unenforceable because it would have required the members of the putative class to travel out of state to litigate "the relatively nominal individual sums at issue"). 

In the arbitration context, however, some California appellate courts have not followed Smith, Valentino and its progeny, but rather have considered expense and inconvenience caused by a forum selection clause and concluded that these factors made the clause unconscionable. Aral v. EarthLink, Inc., for example, held that a forum selection clause requiring California customers of an internet service provider to arbitrate their claims in Georgia was unreasonable. See 134 Cal.App.4th 544, 561, 36 Cal.Rptr.3d 229 (Cal. Ct. App. 2005). The appellate court held that there may be a large number of "consumers who have suffered losses in the range of $40 to $50" but that "to expect any or all of them to travel to Georgia" was "unreasonable as a matter of law." Id. For much the same reasons, Bolter held that a forum selection clause requiring "Mom and Pop" franchisees to arbitrate disputes in Utah was unconscionable. 87 Cal.App.4th at 909, 104 Cal.Rptr.2d 888; see also Magno v. Coll. Network, Inc., 1 Cal.App.5th 277, 288, 204 Cal.Rptr.3d 829 (2016) (same).

To the extent the state appellate courts apply different standards in arbitration and nonarbitration contexts, upholding forum selection clauses in the nonarbitration context (even in adhesion contracts) without considering expense and inconvenience, while striking them down in the arbitration context due to expense and inconvenience, these cases are not binding on us as California law. We reach this conclusion because Sanchez has confirmed that California’s "unconscionability standard is, as it must be, the same for arbitration and nonarbitration agreements." 61 Cal.4th at 912, 190 Cal.Rptr.3d 812, 353 P.3d 741; see also Perry, 482 U.S. at 492 n.9, 107 S.Ct. 2520 ("A court may not ... construe [an arbitration] agreement in a manner different from that in which it otherwise construes nonarbitration agreements under state law."). In determining whether the California Supreme Court would adopt the rule in Smith, Valentino or in Bolter, we are guided by the fact that Sanchez mentioned Smith, Valentino with approval as exemplary of how to determine unconscionability of forum selection clauses. See 61 Cal.4th at 912, 190 Cal.Rptr.3d 812, 353 P.3d 741. Further, the rule in Bolter would be grossly overbroad if applied to all contracts: it could invalidate any forum selection clause in any consumer contract used by a company to sell moderately priced goods in more than one state. Such a rule would clearly contravene California’s general policy preference for the enforcement of forum selection clauses. See Net2Phone, 109 Cal.App.4th at 588. 135 Cal.Rptr.2d 149; Wimsatt v. Beverly Hills Weight Loss Clinics Int'l, Inc., 32 Cal.App.4th 1511, 1523, 38 Cal.Rptr.2d 612 (Cal. Ct. App. 1995).

Here, plaintiffs have not met their burden of proving that the forum selection clause in the Terms of Service is unreasonable. San Francisco is not "unavailable or unable to accomplish substantial justice." Smith, Valentino, 17 Cal.3d at 494, 131 Cal Rptr. 374, 551 P.2d 1206. San Francisco is the principal place of business of 23andMe and so it has a sufficient nexus to the contract. See Polimaster Ltd. v. RAE Sys., Inc., 623 F.3d 832, 837 (9th Cir. 2010). Furthermore, the forum selection clause provided adequate notice that the consumers were agreeing to arbitrate in San Francisco. See Interstaff, 104 Cal.App.4th at 201-02, 127 Cal.Rptr.2d 847. Although plaintiffs submitted two affidavits stating that the cost of traveling to San Francisco for arbitration would be burdensome and expensive, "[m]ere inconvenience or additional expense" does not make the locale unreasonable. Smith, Valentino, 17 Cal.3d at 496, 131 Cal.Rptr. 374, 551 P.2d 1206 (citing M/S Bremen v. Zapata Off-Shore Co., 407 U.S. 1, 16-18, 92 S.Ct. 1907, 32 L.Ed.2d 513 (1972)).

Moreover, even if California courts continue to consider expense and inconvenience in their unconscionability analysis in some circumstances, the plaintiffs have not demonstrated that San Francisco will be "so gravely difficult and inconvenient that [the plaintiffs] will for all practical purposes be deprived of [their] day in court," Aral, 134 Cal.App.4th at 561, 36 Cal. Rptr.3d 229 (quoting M/S Bremen, 407 U.S. at 18, 92 S.Ct. 1907); see Nagrampa, 469 F.3d at 1290 & n.13. The two affidavits submitted by plaintiffs do not provide any detail regarding why the expense of traveling to San Francisco would be too burdensome. Seven of the plaintiffs in this consolidated action reside in California, and, as the district court noted, six of the nine actions in this case were filed
in California. All cases were voluntarily transferred to San Jose, California. Accordingly, we conclude that the forum selection clause is not unconscionable.

C

Finally, we consider the arbitration clause's provision exempting "any disputes relating to intellectual property rights, obligations, or any infringement claims" from mandatory arbitration. The plaintiffs argue that this clause is substantively unconscionable because 23andMe is more likely to bring intellectual property claims against its customers than vice versa, and therefore 23andMe has reserved for itself the advantages of a judicial forum while forcing customers to use the arbitral forum. This argument is based on the assumption that an arbitral forum is inferior to a judicial forum for resolving disputes.

Such a theory finds some support in California law. In Armendariz, the California Supreme Court held that an arbitration provision in an employment agreement was unconscionably unilateral (and thus unenforceable) because, among other things, it required the employee to arbitrate all wrongful termination claims against the employer but gave the employer a choice of forums for its claims. 24 Cal.4th at 120, 99 Cal.Rptr.2d 745, 6 P.3d 669. Armendariz explained that "[g]iven the disadvantages that may exist for plaintiffs arbitrating disputes, it is unfairly one-sided for an employer with superior bargaining power to impose arbitration on the employee as plaintiff but not to accept such limitations when it seeks to prosecute a claim against the employee." Id. at 117, 99 Cal.Rptr.2d 745, 6 P.3d 669. Armendariz emphasized, however, "that if an employer does have reasonable justification for the arrangement," and the arbitration agreement contained a "modicum of bilaterality," in the context of the "business realities" surrounding the contract's formation, it would not be unconscionable. Id. at 117-18, 99 Cal.Rptr.2d 745, 6 P.3d 669.

The California Supreme Court has since clarified Armendariz's reasoning on this issue in several ways. First, the California Supreme Court has backed away from Armendariz's assumptions regarding the inferiority of the arbitral forum. Instead, Sonic II stated that "California and federal law treat the substitution of arbitration for litigation as the mere replacement of one dispute resolution forum for another, resulting in no inherent disadvantage." 57 Cal.4th at 1152, 163 Cal.Rptr.3d 269, 311 P.3d 184. This conclusion is consistent with the Supreme Court cases holding that a state court cannot "rely on the uniqueness of an agreement to arbitrate as a basis for a state-law holding that enforcement would be unconscionable." Concepcion, 563 U.S. at 341, 131 S.Ct. 1740 (quoting Perry, 482 U.S. at 492 n.9, 107 S.Ct. 2520), as well as with our decisions, see Ferguson, 733 F.3d at 936 (holding that the California Supreme Court's reliance "on the institutional advantages of the judicial forum" as the basis for its rule that claims for public injunctive relief could not be arbitrated was inconsistent with Concepcion.), and that of the Tenth Circuit, see THI of N.M. at Hobbs Ctr., LLC v. Patton, 741 F.3d 1162, 1167 (10th Cir. 2014) (holding that the FAA preempts state common law "that is predicated on the view that arbitration is an inferior means of vindicating rights").

Second, the California Supreme Court has confirmed that a one-sided contract is not necessarily unconscionable. "[A] contract can provide for a margin of safety that provides the party with superior bargaining strength a type of extra protection for which it has a legitimate commercial need without being unconscionable." Baltazar, 62 Cal.4th at 1250, 200 Cal.Rptr.3d 7, 367 P.3d 6 (internal quotation marks omitted). Along these lines, Sanchez upheld two provisions in a contract between a car buyer and a car dealership that were alleged to be more favorable to the stronger party. Sanchez, 61 Cal.4th at 916, 190 Cal.Rptr.3d 812, 353 P.3d 741. The first provision forbade appeals of an arbitral decision unless it reached a specific dollar threshold. Sanchez concluded that this provision was not unconscionable because "the appeal threshold provision does not, on its face, obviously favor the drafting party." Id. at 916, 190 Cal.Rptr.3d 812, 353 P.3d 741. The second provision provided that "only arbitral grants of injunctive relief" were subject to a second arbitration. Id. at 917, 190 Cal.Rptr.3d 812, 353 P.3d 741. Although acknowledging that "overall the car buyer is more likely than the seller to seek injunctive relief," Sanchez held that the one-sided nature of this provision did not render it unconscionable because the extra margin of safety provided by the clause was reasonable given "the broad impact that injunctive relief may have on the car seller's business." Id. Similarly, Baltazar v. Forever 21, Inc, held that a provision that "compelled arbitration of all employment-related claims, while permitting both parties to seek injunctive relief" in a preliminary court proceeding was not unreasonably unconscionable even if the employer was "practically speaking" more likely to seek the remedy of preliminary injunctive relief. 62 Cal.4th at 1248 & n.4, 200 Cal.Rptr.3d 7, 367 P.3d 6.

Under this precedent, the provision in the Terms of Service in this case excluding intellectual property claims from mandatory arbitration is not unconscionable. As in Sanchez, the provision in this case exempting "any disputes relating to intellectual property rights, obligations, or any infringement claims" from mandatory arbitration "does not, on its face, obviously favor the drafting party." 61 Cal.4th at 916, 190 Cal.Rptr.3d 812, 353 P.3d 741. Under the Terms of Service, customers retained certain intellectual property rights, including rights in user-generated content and genetic information. The customers would be able to bring claims against 23andMe based on these rights in court. Conversely, the plaintiffs have not identified any intellectual property rights claims that
23andMe are likely to bring against its customers. Even under Armendariz, the intellectual property provision has more than a “modicum of bilaterality.” Armendariz, 24 Cal.4th at 117, 99 Cal.Rptr.2d 745, 6 P.3d 669. Moreover, to the extent 23andMe has valuable intellectual property rights in its website and database, it is entitled to an extra “margin of safety” based on legitimate business needs. Baltazar, 62 Cal.4th at 1250, 200 Cal.Rptr.3d 7, 367 P.3d 6. We therefore conclude plaintiffs have not carried their burden of demonstrating that the intellectual property exemption is unconscionable under current California law.

D

1032

Plaintiffs also challenge a provision in the Terms of Service establishing a one-year statute of limitations period and a provision giving 23andMe a unilateral right to modify the agreement. These provisions are not contained within the arbitration clause itself.

Because §2 of the FAA states that an agreement to arbitrate is “valid, irrevocable, and enforceable,” and does not address “the validity of the contract in which it is contained,” the United States Supreme Court has held that “a party’s challenge to another provision of the contract, or to the contract as a whole, does not prevent a court from enforcing a specific agreement to arbitrate.” Rent-A-Center, W., Inc. v. Jackson, 561 U.S. 63, 70-71, 130 S.Ct. 2772, 177 L.Ed.2d 403 (2010). In other words, if the plaintiff does not specifically and directly challenge the “precise agreement to arbitrate at issue,” id. at 71, 130 S.Ct. 2772, a court must treat the arbitration agreement as valid under §2 and enforce it, thereby letting the arbitrator decide questions as to the validity of other provisions in the first instance, id. at 72, 130 S.Ct. 2772. This rule applies even when the plaintiff challenges the contract on “a ground that directly affects the entire agreement (e.g., the agreement was fraudulently induced), or on the ground that the illegality of one of the contract’s provisions renders the whole contract invalid.” Buckeye Check Cashing, Inc. v. Cardegna, 546 U.S. 440, 444, 126 S.Ct. 1204, 163 L.Ed.2d 1038 (2006). Given this precedent, our authority to review portions of the contract outside the arbitration provision is limited. But as Rent-A-Center indicates, “[I]t may be that” where a plaintiff challenges “the validity under §2 of the precise agreement to arbitrate at issue” on the ground that certain general contract provisions “as applied” to the agreement to arbitrate render it unconscionable, such a “challenge should [be] considered by the court.” 561 U.S. at 71, 74, 130 S.Ct. 2772 (emphasis in original). Cf. Nagrampa, 469 F.3d at 1276 (holding a court’s determination whether an arbitration agreement is procedurally unconscionable may be informed by consideration of the contract as a whole).

Turning first to the one-year statute of limitations, we conclude that it does not make the arbitration provision itself unconscionable under California law. The leading California case on this issue is Moreno v. Sanchez, 106 Cal App.4th 1415, 131 Cal. Rptr.2d 684 (Cal. Ct. App. 2003), which was cited by the California Supreme Court in Sanchez v. Valencia as exemplifying the application of California’s unconscionability doctrine to statute of limitations clauses. 61 Cal.4th at 912, 190 Cal. Rptr.3d 812, 353 P.3d 741. Moreno explained that California courts “have afforded contracting parties considerable freedom to modify the length of a statute of limitations.” Id.; see also Han v. Mobil Oil Corp., 73 F.3d 872, 877 (9th Cir. 1995) (“A contractual limitation period requiring a plaintiff to commence an action within 12 months following the event giving rise to a claim is a reasonable limitation which generally manifests no undue advantage and no unfairness.”). Moreover, California courts generally interpret contractual statute of limitations as incorporating California’s discovery rule, in order to avoid unfair or unreasonable applications of the limitations period. Moreno, 106 Cal. App.4th at 1430, 131 Cal.Rptr.2d 684. Nor is the statute of limitations in the Terms of Service in this case unfairly one-sided; the provision by its terms, applies to claims brought by both parties. Compare Pokorny, 601 F.3d at 1001 (holding that a unilateral clause shortening the limitations period added to the unconscionability of the contract). Accordingly, the statute of limitations provision does not make the arbitration provision unconscionable.

Likewise, under the circumstances here, the unilateral modification clause does not make the arbitration provision itself unconscionable. California courts have held that the implied covenant of good faith and fair dealing prevents a party from exercising its rights under a unilateral modification clause in a way that would make it unconscionable. See, e.g., Casas v. Carmax Auto Superstores Cal, LLC, 224 Cal.App.4th 1233, 1237, 169 Cal.Rptr.3d 96 (Cal. Ct. App. 2014); see also, e.g., Cobb v. Ironwood Country Club, 233 Cal.App.4th 960, 965-66, 183 Cal.Rptr.3d 282 (Cal. Ct. App. 2015). Although we have held that a unilateral modification provision itself may be unconscionable, see Ingle v. Circuit City Stores, Inc., 328 F.3d 1165, 1179 (9th Cir. 2003), we have not held that such an unconscionable provision makes the arbitration provision or the contract as a whole unenforceable. Id. at 1179 n.23. We conclude that plaintiffs have not carried their burden of demonstrating that the unilateral modification provision renders the arbitration clause, set forth in a separate provision, unconscionable. While plaintiffs are free to argue during arbitration that the unilateral modification clause itself is unenforceable, we do not reach this claim here. See Kilgore v. KeyBank, Nat. Ass’n, 718 F.3d 1052, 1059 n.9 (9th Cir. 2013) (en banc).
IV

We conclude that under principles established by recent California Supreme Court decisions, California's common law rule of unconscionability does not provide a basis to revoke the arbitration agreement in the Terms of Service here. Accordingly, the arbitration agreement is "valid, irrevocable, and enforceable." 9 U.S.C. § 2.

AFFIRMED.

WATFORD, Circuit Judge, concurring in the judgment:

I agree with the majority that the arbitration provision is valid and enforceable, albeit for different reasons. Like the district court, I see no need to address whether the fee-shifting clause is substantively unconscionable because 23andMe has waived its right to enforce that clause — a clause that would have been severable in any event. As for the venue-selection clause, it cannot be deemed substantively unconscionable as to these plaintiffs. Three of the class actions involved in this appeal were filed in the District Court for the Northern District of California, and the plaintiffs in each of the other class actions voluntarily transferred their actions to that court. So, provided the cases can proceed on a class-action basis, it seems obvious that litigating in an arbitral forum in San Francisco will not pose any undue hardship for the plaintiffs. At oral argument, 23andMe conceded that these cases may proceed as class arbitrations (the arbitration provision does not contain a class-action waiver), and the rules of the arbitration provider designated by the parties specifically provide for class arbitration. Finally, the arbitration provision's carve-out for intellectual property claims is not so one-sided as to be substantively unconscionable. The plaintiffs have not shown that intellectual property claims represent the claims that 23andMe would be most likely to assert against consumers and that consumers would be least likely to assert against 23andMe.

I would not address the remaining two clauses — the 1-year limitations period and the unilateral modification clause — because the plaintiffs have challenged those two clauses only insofar as they aggravate the supposed substantive unconscionability of the other three clauses.


A written provision in any maritime transaction or a contract evidencing a transaction involving commerce to settle by arbitration a controversy thereafter arising out of such contract or transaction, or the refusal to perform the whole or any part thereof, or an agreement in writing to submit to arbitration an existing controversy arising out of such a contract, transaction, or refusal, shall be valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract.

[2] The parties do not dispute the court's finding that the Terms of Service were procedurally unconscionable, and thus we do not address that question.

[3] Section 1717 of the California Civil Code states, in full:

In any action on a contract, where the contract specifically provides that attorney's fees and costs, which are incurred to enforce that contract, shall be awarded either to one of the parties or to the prevailing party, then the party who is determined to be the party prevailing on the contract, whether he or she is the party specified in the contract or not, shall be entitled to reasonable attorney's fees in addition to other costs.

[4] Because Section 1284.3 is applicable only in the arbitration context, there is a question whether it would be preempted by the FAA if used to invalidate a fee-shifting clause. We need not reach this issue, however, because we determine that the fee-shifting provision in this case is not unconscionable under existing California law.

[5] Although we previously applied the Armendariz rule in the context of a consumer agreement, Ting, 319 F.3d at 1135, we are bound by the California Supreme Court's subsequent opinion in Sanchez. See In re Watts, 298 F.3d 1077, 1082-83 (9th Cir. 2002) (holding that our interpretation of a state law issue "was only binding in the absence of any subsequent indication from the California courts that our interpretation was incorrect," and we are bound to follow the rationale California Supreme Court would likely follow).

[6] Although we followed Aral and Bolter's approach to forum selection clauses in Nagrampa, 469 F.3d at 1288-90, we did not have guidance from Sanchez at that time. Sanchez has since barred state courts from applying an unconscionability doctrine in a different manner in arbitration and nonarbitration contexts. 61 Cal.4th at 912, 190 Cal.Rptr.3d 812, 353 P.3d 741. Because Aral and Bolter both adopted an arbitration-specific approach to determining the unconscionability of a forum selection clause, we must reconsider the current state of California law in light of Sanchez. See In re Watts, 298 F.3d 1077, 1082-83 (9th Cir. 2002).

[7] In oral argument, the plaintiffs asserted that 23andMe is building a database of genetic information based on its customers' DNA results and that 23andMe might resort to copyright law to prevent customers from publishing the DNA data of other customers. (Customers are allowed to publish their own data under the agreement.) There is no support in the record for this assertion, and it appears to be purely speculative. Therefore, it does not support the plaintiffs' argument that 23andMe is more likely to bring intellectual property claims than consumers.

[8] Section 28(d) states:
Term for cause of actions. You agree that regardless of any statute or law to the contrary, any claim or cause of action arising out of or related to use of the Services or the TOS must be filed within one (1) year after such claim or cause of action arose or be forever barred.

Paragraph 26, entitled "Changes to the Terms of Service" states:

23andMe may make changes to the TOS [terms of service] from time to time. When these changes are made, 23andMe will make a new copy of the TOS available on its website and any new additional terms will be made available to you from within, or through, the affected services.

You acknowledge and agree that if you use the Services after the date on which the TOS have changed, 23andMe will treat your use as acceptance of the updated TOS.

Save trees - read court opinions online on Google Scholar.
FDA Approves 23andMe’s At-Home DNA Tests for 10 Diseases
by MAGGIE FOX

The Food and Drug Administration approved the first home DNA tests Thursday that let people find out if they have a genetic risk for certain diseases.

The FDA decision allows home DNA test company 23andMe to directly market its gene tests for 10 diseases, including Parkinson’s, Alzheimer’s and some rare blood diseases.

“These are the first direct-to-consumer (DTC) tests authorized by the FDA that provide information on an individual’s genetic predisposition to certain medical diseases or conditions, which may help to make decisions about lifestyle choices or to inform discussions with a health care professional,” the FDA said in a statement.

“Consumers can now have direct access to certain genetic risk information,” said Dr. Jeffrey Shuren, director of the FDA’s Center for Devices and Radiological Health, which approves these kinds of tests.

“But it is important that people understand that genetic risk is just one piece of the bigger puzzle. It does not mean they will or won’t ultimately develop a disease.”

Related: Stop Selling Home DNA tests, FDA Tells 23andMe

A person’s genes almost never make for a 100 percent risk of any disease. Instead, many different genes usually interact with a person’s lifestyle and other factors to cause disease. For instance, the National Institute on Aging (NIA) notes that many genes are involved in developing Alzheimer’s disease, and it’s not clear how much each one raises the risk.

Related: 23andMe Faces Class Action Lawsuit in California

“It is unlikely that genetic testing will ever be able to predict the disease with 100 percent accuracy, researchers believe, because too many other factors may influence its development and progression,” the NIA, one of the National Institutes of Health, says on its website.

“It does not mean they will or won’t ultimately develop a disease.”

And some genetic mutations are inherited, some develop before birth, and some occur as people live their lives. How, where and when these changes develop can affect whether such changes causes disease.
Samples are prepared for DNA testing at the Genetic Institute Nantes-Atlantique (IGNA) on Dec. 10, 2015 in Nantes, western France. Home DNA testing company 23andMe got a go-ahead from the FDA to market a home genetic test for 10 diseases. Georges Gobet / AFP-Getty Images

The FDA's decision, which is sure to stir up controversy, is a big turnaround from 2013, when the FDA singled out 23andMe, ordering the company to stop marketing its over-the-counter gene test.

23andMe is especially aggressive in marketing its home tests, usually offered as saliva tests that customers can send in for analysis.

This test does not include checks for genes that predispose people to cancer. They look instead for DNA variation involved in 10 conditions:

- Parkinson’s disease
- Late-onset Alzheimer’s disease
- Celiac disease, which causes the inability to digest gluten.
- Alpha-1 antitrypsin deficiency, a disorder that raises the risk of lung and liver disease. More than 100 different genetic variations of the gene have been identified and only some are linked with deficiency.
- Early-onset primary dystonia, a movement disorder involving involuntary muscle contractions and other uncontrolled movements.
- Factor XI deficiency, a blood clotting disorder caused by certain mutations in a gene called F11.
- Gaucher disease type 1, an organ and tissue disorder caused by mutations in the GBA gene.
- Glucose-6-Phosphate Dehydrogenase deficiency, also known as G6PD, a red blood cell condition.
- Hereditary hemochromatosis, an iron overload disorder caused by mutations in at least five different genes.
- Hereditary thrombophilia, a blood clot disorder.

The FDA says these are all serious conditions and customers must first click an acknowledgement that they understand the results could cause them anxiety, a spokeswoman said. “The ‘opt-in’ page includes links to recommendations from professional medical associations on the benefits and risks of genetic testing for users to read before deciding whether to receive test results,” the FDA spokeswoman, Tara Goodin, said via email.

New York University bioethicist Art Caplan says he is surprised the FDA approved the home tests, given the questions that still surround even genetic tests done by physicians.

Related: Mutant Gene Protects Against Heart Attack
```
"So much remains unknown, both about the accuracy of testing and the ability of consumers to process genetic information without counseling or help," Caplan said.

"Even physicians have a difficult time knowing how to interpret genetic test risk information. So this decision may wind up frightening as many people about genetic risk as it does empower them."

Kathy Hibbs, chief legal officer at 23andMe, said the company had changed the tests to address those issues.

"We had to conduct studies to show that consumers drawn from abroad swath of society could understand and use the product appropriately," Hibbs told NBC News. "We call those ‘user comprehension’ studies. We conducted those and submitted them to FDA to demonstrate that Americans can access and understand and use the product in a safe and effective way."

Hibbs says the tests will explain that having -- or lacking -- a genetic predisposition to a disease does not make for perfect certainty. "We provide information on how to access genetic counseling, although we don’t provide genetic counseling ourselves," she said.

“**Even physicians have a difficult time knowing how to interpret genetic test risk information.**”

And the FDA says the test will recommend that customers "speak with a healthcare professional, genetic counselor, or equivalent professional before getting the results of the test."

Medical geneticist Dr. Robert Green of Harvard University said people who buy the test tend to understand the risks. "We’re moving as a society toward empowering people with health related information and this is, I think, a welcome step, along that journey," Green said.

Caplan says it's also not clear what privacy people have and how well 23andMe could safeguard their test results, or even their actual samples.

**Related: How Much Cancer is Due to Genes?**

The FDA said it reviewed the tests through a new process.

Consumers can expect more such tests to hit the market now.

“In addition, the FDA intends to exempt additional 23andMe genetic health risk tests from the FDA's premarket review, and genetic health risk tests from other makers may be exempt after submitting their first premarket notification,” the FDA said.

“A proposed exemption of this kind would allow other, similar tests to enter the market as quickly as possible and in the least burdensome way, after a one-time FDA review.”
```
Concerned about connected car privacy? Bluetooth sensors used to track traffic

Bluetooth signals from cars provide an accurate record of real-time traffic patterns.

JONATHAN M. GITLIN - 7/24/2017, 8:20 AM

One big promise of the connected car revolution has been the potential to help clear up traffic problems. When every vehicle and traffic signal is connected to the cloud, municipalities and local governments should be able to have a constant view of the traffic on their streets, aware of any problems almost instantly. The catch? It's going to take a long time before there are sufficient vehicle-
to-infrastructure (V2I) or even vehicle-to-vehicle (V2V)-equipped cars on our roads. But the city of Aarhus in Denmark has shown you don't need to wait for V2x to finally penetrate the market to start doing that; all you need are outdoor Bluetooth sensors.

For some time, Aarhus has been using Bluetooth sensors to collect traffic pattern information. As people drive around, emitting Bluetooth signals, the sensors log their movements around the city. In doing so, their traffic patterns can flag and reveal problems that the city needs to fix.

"The benefits we have gained from the solution since implementation are very significant. We now discover errors and irregularities that we would not have a chance to see otherwise. In addition, it is extremely educational and easily accessible to study how the incidents of various kinds influence the road network," says Asbjørn Halskov-Sørensen, ITS Project Manager at Aarhus Municipality.

"Ultimately, the data contributes to an improved economy and a better environment through
Qualcomm throws down a marker to other connected cars

Connected cars aren’t just for hacking

Tech firms want to save the auto industry—and the connected car—from itself

Hate driving to the gas station? Meet Volvo’s new connected concierge service
Smart Cities, Copenhagen and the Power of Data
In Copenhagen, smart street lights dim during a full moon and brighten when cyclists and walkers pass below. Video surveillance systems help keep citizens safe. Internet of Things sensors ward off water pipe leaks, while wind turbines power buildings. Fire-fighting drones stand ready.

It’s a smart city getting smarter every day, thanks to data gathered by IoT sensors.

Many government officials have heard about Copenhagen’s success and now dream of a smart city, too. According to CompTIA, one out of 10 government entities has a formal IoT initiative underway, and one out of four has a pilot project in the works.

“A Jetsons-like future seems increasingly within reach,” says Tim Herbert, senior vice president of research and market intelligence at CompTIA, in a research brief.

Smart cities offer lots of advantages, both today and in the future. Automated operational processes lead to tangible cost savings. A smart city churns out an awesome amount of data, which can be analyzed and used to make quick decisions, cutting through layers of city bureaucracy. Best of all, a smart city attracts the kind of tech-savvy millennial to live and work, thus raising the city’s profile.


Only about 1,000 of the nearly 20,000 cities and towns in the United States have some type of IoT or smart city initiative underway, CompTIA says. That’s still a lot of investment dollars in play. McKinsey predicts the global smart cities component of the IoT market will range between $930 billion to $1.7 trillion by 2025.
Copenhagen aside, U.S. cities such as Houston, New York and Columbus, Ohio, have made strides to become smart cities. Columbus, in particular, has become a poster child for the smart city. This summer, U.S. Department of Transportation awarded $40 million to Columbus as the winner of its Smart City Challenge. Now Columbus has designs on electric self-driving shuttles, vehicle-to-vehicle data and smart traffic lights that keep traffic flowing.

Related: San Antonio Proposes $13 Million Smart Cities Initiatives

Budget

So why aren’t more city managers and elected officials joining the smart city movement? Technical complexity and political challenges keep many on the sidelines. CompTIA cites a laundry list of major concerns: cyber-security risks, a data privacy backlash, unforeseen regulations, lack of IoT-skilled workers, upfront investment costs, interoperability issues, elusive returns on investment, and an inability to take advantage of new data streams.

“Realistically, though, decisions regarding whether to proceed with smart cities initiatives will be contingent on outputs rather than inputs,” Herbert says. “Smart city investments will be judged by metrics such as improvement to livability, cost savings, citizen engagement, business community support, and votes at the ballot box.”

Related: Channel Stakes Out IoT

In order to simplify things, CompTIA eyes a new solution emerging from the channel – “smart cities as a service.” Imagine a packaged solution combining integration, data, security and cloud computing in a scalable, standardized way. It would make the decision to start down the road to the smart city much easier.

“The ‘smart cities-as-a-service’ approach brings it all together into what many city planners will view as an appealing option,” Herbert says.
Tom Kaneshige is editor of Five2ndWindow, an independent news channel that is part of Internet of Things Institute covering mobile, IoT, marketing and the digital enterprise. You can reach him at tom.kaneshige@penton.com.

Acting Federal Trade Commission (FTC) Chairman Maureen K. Ohlhausen made it clear that she expects the FTC’s enforcement role in protecting privacy and security to encompass automated and connected vehicles. In her opening remarks at a June 28, 2017 workshop hosted by the FTC and National Highway Traffic Safety Administration (NHTSA), she said the FTC will take action against manufacturers and service providers of autonomous and connected vehicles if their activities violate Section 5 of the FTC Act, which prohibits unfair and deceptive acts or practices.

Such concern is warranted as new technologies allow vehicles not only to access the Internet, but also to independently generate, store and transmit all types of data – some of which could be very valuable to law enforcement, insurance companies, and other industries. For example, such data can not only show a car’s precise location, but also whether it violated posted speed limits, and aggressively followed behind, or cut-off, other cars.

Acting Chairman Ohlhausen noted that the FTC wants to coordinate its regulatory efforts with NHTSA, and envisions that both organizations will have important roles, similar to the way the FTC and the Department of Health and Human Services both have roles with respect to the Health Insurance Portability and Accountability Act (HIPAA).

Traditionally, NHTSA has dealt with vehicle safety issues, as opposed to privacy and data security. Thus, it may mean that the FTC will have a key role on these issues as they apply to connected cars, as it already has been a major player on privacy and data security in other industries.

Acting Chairman Ohlhausen also encouraged Congress to consider data breach and data security legislation for these new industries, but speakers at the workshop (video available here) noted that legislation in this area will have difficulty keeping up with the fast pace of change of these technologies.
Specific federal legislation, or even laws at the state level, may be slow in coming given the many stakeholders who have an interest in the outcome. Until then, the broad mandate of Section 5 may be one of the main sources of enforcement. Companies who provide goods or services related to autonomous and connected vehicles should be familiar with the basic FTC security advice we have already blogged about here, and should work with knowledgeable attorneys as they pursue their design and manufacture plans.

[View source.]
A MURDER CASE TESTS ALEXA’S DEVOTION TO YOUR PRIVACY

THE AMAZON ECHO can seem like your best friend—until it betrays you. That's because this device is different from anything else in your house. Alexa, the voice assistant that powers Echo and more, is always listening, sending what you say after using a "wake" word to Amazon's servers. Of course, Echo isn't the only voice-assistant speaker on the market, but it sits in millions of homes, and Alexa is headed to devices from companies like Ford, Dish, Samsung, and Whirlpool.

Thankfully, before Alexa can betray you, Amazon is taking steps to push back.
Arkansas police recently demanded that Amazon turn over information collected from a murder suspect's Echo. Amazon's attorneys contend that the First Amendment's free speech protection applies to information gathered and sent by the device; as a result, Amazon argues, the police should jump through several legal hoops before the company is required to release your data.

If Amazon has its way, the police must prove the state has a compelling need for the information and that the material can’t be obtained elsewhere (such as from another source—a receipt in a person's possession, for instance). The information sought must be specific and integral to the investigation. If the police meet this test, a judge will review the information in private and decide what information, if any, should be disclosed.

Law enforcement has a well-documented history of expanding investigations into areas that test an individual's right to privacy. The US Supreme Court, in 1967's Katz v. United States, determined that the FBI's use of an electronic eavesdropping device affixed to the outside of a telephone booth was an invasion of privacy, and that the material it collected could not be offered as evidence at trial. That decision demonstrates that there are limits to what the police can do in their investigations and may provide guidance for the Arkansas court in considering Amazon's arguments.

Amazon's effort to protect the data your Echo collects by invoking the First Amendment is commendable, but the company has failed to address the real problem: Why is all that data just sitting in Amazon's servers in the first place? The brief Amazon filed in the Arkansas court confirms that the company saves the recordings and transcripts of your dialogue with Alexa on servers where "all data is protected during transmission and securely stored." So should we just trust that Amazon's servers are impenetrable?

Digital assistants like the Echo and Google Home are backed by sophisticated cloud-based artificial intelligence systems, connected to your home through the internet to at least one speaker and an always-on microphone. Use the right trigger phrase, and the digital assistant is all ears, ready to do your bidding: streaming music, answering questions, controlling smart-home devices, scheduling events and, especially for Amazon, buying things.

Think of the assistants like really smart dogs. They're always ready to react to specific commands. Also like a really smart dog, they can remember those commands forever. And
this concept of an always-on, always-connected, always-remembering listening device is where it gets intriguing.

Amazon argues that Alexa only records when the trigger word is spoken, and users can mute the device by pressing a button. But consider this: In the Oscar-winning documentary Citizenfour, during a meeting with journalists Laura Poitras and Glenn Greenwald, Edward Snowden disconnects a landline phone in the hotel room because it might be used as a listening device.

Mobile phones, computer webcams and now, digital assistants also can be co-opted for nefarious purposes. These are not potential listening devices. They are listening devices—that's why they exist. And if a hotel-room phone can be rigged as a listening device for other than its original purposes, why not something built to listen all the time?

Let's look at a few scenarios. These are more or less specific to Amazon's technology and policies, but variants could apply to Google Home or other digital assistants.

---

**RELATED STORIES**

**BRIAN BARRETT**
Amazon Alexa Hits 10,000 Skills. Here Comes the Hard Part

**TIM MOYNIHAN**
OK, Alexa: A Google Home Versus Amazon Echo IQ Test

**TIM MOYNIHAN**
Alexa and Google Home Record What You Say. But What Happens to That Data?

---

Say you're meeting with your attorney, confess you've had an affair with a woman named Alexa, and happen to say the trigger phrase (after all, more than 100,000 people born in the past 25 years were given that name). Who has access to that recording? Or what if, in a meeting, someone triggers the device to record the conversation without your permission? This would be legal, if unethical, in so-called one-party consent states (California requires permission from both parties before recording).
This brings up a more basic question: Do you have to give informed consent to be recorded each time you enter my Alexa-outfitted home? Do I have to actively request your permission? And who, at Amazon or beyond, gets to see what tendencies are revealed by your Alexa commands? Amazon claims you can permanently delete the voice recordings, though wiping them degrades performance. Even if you're smart enough to clear your browser history, are you smart enough to clear this, too? And what about the transcripts?

Another question: How do you know when your digital assistant is recording what you say? Amazon provides several ways to activate the recording beyond the "wake" word. A light on the Echo turns blue to indicate audio is streaming to the cloud. After the request is processed, the audio feed is supposed to close. You can also set the device to play a sound when it stops streaming your audio, but what happens if the device is hacked or modified to keep recording?

There are endless scenarios where digital assistants could be problematic. Current law, as always with fast-emerging technologies, will struggle to catch up. Amazon's contentions in the Arkansas criminal case, overall, offer a good start for setting some legal standards.

And of course these issues apply beyond Amazon and Alexa. In fact, they may be more problematic with Google Home and other competitors. Among other things, Google Home has access to your private calendar—it knows the events that you feel were important enough to flag for a particular day.

Google's privacy policies and other online materials about Home don't directly address voice-recorded issues. But its policies do say, "Google will share your information with companies, organizations, and individuals outside of Google if Google has a good-faith belief that access, use, preservation, or disclosure of the information is reasonably necessary to meet applicable law, regulation, legal process, or enforceable government request." In short, it appears that Google doesn't ask for your permission to share your voice recordings.

And yes, you can delete your search history in Google Home, but like Amazon, the company says doing so "will limit the personalized experience for features like the Google Assistant."

Millions of people are putting digital assistants in their lives with no clue about the potential havoc this Trojan horse could bring. Based on what Amazon and Google say about their devices, everyone needs to recognize the unresolved legal issues involving this new technology. Beware of who, or what, is listening.
Why EULAs suck for the Internet of Things

May 30, 2014 in Business, Ideas, infrastructure, Internet, IoT, Personal, Personal clouds, problems, Technology, VRM | 1 comment

I’ve been asked how EULAs — End User License Agreements (http://en.wikipedia.org/wiki/End-user_license_agreement) — might affect the Internet of Things, now becoming better known as the IoT (http://en.wikipedia.org/wiki/Internet_of_Things). Good question. The topic is hot:

(https://www.google.com/trends/explore?q=%22Internet%20of%20Things%22)

Development, however, is another story. There we are headed straight into a log-jam that Phil Windley (http://windley.com) calls the Compuserve of Things (http://bit.ly/1fxCLlp). In the 80’s and early ’90s, Compuserve (http://en.wikipedia.org/wiki/CompuServe) was as close as any of us could get to experiencing the real Internet (which was available only to a limited selection of governments, universities and big companies). Compuserve’s competitors were AOL (originally America OnLine (http://en.wikipedia.org/wiki/AOL), Prodigy (http://en.wikipedia.org/wiki/The_Prodigy), MSN (http://en.wikipedia.org/wiki/MSN) and a few others not worth mentioning.

The problem was that all online services were closed and proprietary. Communication between them was difficult or impossible. Your Compuserve email only worked with other Compuserve members. Same with your Prodigy and AOL mail. Same with instant messaging (which retains its old proprietary problems even to this day.)

Where we are headed today is not the Internet of Things, but the Google of Things (http://techcrunch.com/2014/01/27/google-is-making-a-land-grab-for-the-internet-of-things/), the Apple of Things (http://www.forbes.com/sites/rogerkay/2014/05/27/will-apple-play-nice-on-the-internet-of-things/), the Microsoft of Things, and low-effort sports and war stories (http://tech.fortune.cnn.com/2014/05/27/apple-google-smart-house/) in the media misdirecting attention away from the real Internet and toward fights between giants.

Also evolving away from the Net will be the Every-BigCo-of-things, and their suppliers (http://www.fool.com/investing/general/2014/05/29/meet-jasper-a-company-powering-the-internet-of-thi.aspx) of proprietary platforms.
(Let's call that one EBCoT.) Every one of these, of course, will have its own EULA.

The Internet has no EULA. It just has an A, for Agreement (http://worldofends.com/). That’s because the Internet is defined by protocols (http://en.wikipedia.org/wiki/Internet_protocol_suite), which are manners — agreements — among the things it connects.

For the trillions of things in the world to work in the actual Internet, they need be subject to that same agreement (and others like it, tuned for things other than computers), but not licenses from controlling parties, because that would not be the Internet.

EULAs suck already anyway, for two legacy reasons: 1) they are one-sided and coercive; and 2) nobody reads them other than the lawyers who write them. Let’s unpack both problems.

Most EULAs are what legal folk call "contracts of adhesion. (http://legal-dictionary.thefreedictionary.com/Adhesion+Contract)." That term was coined (http://digitalcommons.law.yale.edu/fss_papers/2731/) by Friedrich Kessler (http://en.wikipedia.org/wiki/Friedrich_Kessler) in 1943, at the apex of the Industrial Age (when Industry was causing, fighting and winning WWII). Adhesive contracts, Kessler said, were the only way any one company could achieve legal scale with masses of customers and users.

But what worked as an upside for industry had a downside for everybody else, because adhesive contracts came at a cost. Freedom of contract (http://en.wikipedia.org/wiki/Freedom_of_contract), long a form of vernacular law in everyday life, was shoved aside by industrial expedience.

What Kessler saw as both an efficient hack and a moral drag became more of both in the Information Age (http://en.wikipedia.org/wiki/Information_Age) in which we live today. And it be a far bigger drag if it encumbers every Thing we want to put on the Internet.

Most of us don’t read EULAs, or the privacy policies that often accompany them, because to do so is both useless and time consuming (http://bit.ly/1nPNZHL). They are useless because they exist mostly to scrape off liability and other inconveniences on the customer or user. And they suck up time because they are written in legalese, by and for lawyers, rather than the rest of us.

So: what can we do? I’ll take that up in the next post.

Bonus link: Tony Faddel on Nest’s independence from Google and why he doesn’t like “Internet of Things” as a label (http://recode.net/2014/05/28/nests-tony-fadell-on-the-internet-of-things-and-apple-video/).

SHARE THIS:

(https://blogs.harvard.edu/doc/2014/05/30/why-eulas-suck-for-the-internet-of-things/?share=linkedin&nb=1)

(https://blogs.harvard.edu/doc/2014/05/30/why-eulas-suck-for-the-internet-of-things/?share=facebook&nb=1)
Medical Devices Hit By Ransomware For The First Time In US Hospitals

Is it possible that North Korea used a stolen National Security Agency hacking tool to infect medical devices at U.S. hospitals? Turns out, in today’s topsy-turvy world, it is.

When the NSA cyber weapon-powered WannaCry ransomware spread across the world this past weekend, it infected as many as 200,000 Windows systems, including those at 48 hospital trusts in the U.K. and so-far unnamed medical facilities in the U.S. too. It wasn’t just administrative PCs that were hacked, though. Medical devices themselves were affected too, Forbes has learned.

A source in the healthcare industry passed Forbes an image of an infected Bayer Medrad device in a U.S. hospital. The source did not say which specific hospital was affected, nor could they confirm what Bayer model was hacked. But it appears to be radiology equipment designed to help improve imaging. More specifically, it’s a device used for monitoring what’s known in the industry as a “power injector,” which helps deliver a “contrast agent” to a patient. Such agents consist of chemicals that improve the quality of magnetic resonance imaging (MRI) scans.
A Bayer spokesperson confirmed it had received two reports from customers in the U.S. with devices hit by the ransomware, but would not say which specific products were affected. “Operations at both sites were restored within 24 hours,” the spokesperson added. “If a hospital’s network is compromised, this may affect Bayer’s Windows-based devices connected to that network.”

Bayer said it would be sending out a Microsoft patch for its Windows-based devices “soon.” The firm recommended hospitals work with their IT security teams and contact Bayer’s Technical Assistance Center “to ensure continued support of contrast-enhanced radiology procedures which use Bayer power injectors.”

As noted by Beau Woods, deputy director of Cyber Statecraft Initiative at the Atlantic Council, ransomware infecting such a device shouldn’t necessarily threaten patient safety directly, other than stopping scanning machines working. “I seriously doubt Windows is controlling any of the safety functions,” he said.

But on Twitter, Woods explained the real impact of such attacks: “Medical device outages increase resource needs, delay care, trigger more clinical mistakes. The harm can go unseen unless you look for it.” Multiple U.K. hospitals reported that their radiology departments were completely knocked out by the ransomware outbreak.

North Korea + NSA exploits = infected hospitals?

Whatever the impact on patient health, the Bayer infections represent the first known instance of ransomware directly affecting the operation of a medical device. They’ve also provided the first evidence that the WannaCry outbreak hit U.S.
healthcare bodies, showing that America’s own powerful intelligence tools have been turned against some of its most sensitive institutions. Not to mention that clues indicate possible North Korean involvement in the attacks.

Cybersecurity firms are developing increasing levels of confidence of North Korean involvement. The WannaCry hackers used tools first leaked by a shady crew called the Shadow Brokers, combining them with code linked to North Korean cyber operations. BAE Systems, a government arms contractor and cyber specialist, said it had found “multiple overlaps” between the WannaCry malware and that controlled by the Lazarus Group, which the firm associated with North Korean activity.

The similarities included common source code that was previously unique to Lazarus, use of the same code compiler, unusual “leetspeak” (a kind of internet language popular amongst certain hacker communities), and both focused on Bitcoin, “presumably for stealing funds and money-laundering,” said Adrian Nish, BAE’s head of threat intelligence.

**Healthcare tech industry on alert**

Meanwhile, in the last 24 hours, some of the world’s biggest healthcare tech companies have rushed out warnings about WannaCry and its impact on their products. Much the same as Bayer, they’re still developing adequate patches to protect systems from another similar attack.

The Health Information Trust Alliance (HITRUST), a privately held company that provides a cyber threat exchange platform for the healthcare industry, said it had reports of both Bayer and Siemens equipment being affected by the outbreak.

Siemens told Forbes it couldn’t confirm or deny reports its Healthineers technologies had been affected. But it publicly stated has been working with the U.K. National Health Service (NHS) to help get systems back online, with engineers deployed across the country to assist.

“Select Siemens Healthineers products may be affected by the Microsoft vulnerability being exploited by the WannaCry ransomware,” the firm wrote in an advisory. The firm is developing
patches or remediation solutions for systems running the vulnerable version of Microsoft's SMB v1, a component in Windows which was originally exploited by an NSA hacking tool known as EternalBlue before the WannaCry perpetrators abused it. It released multiple warnings for different healthcare products, warning they could be susceptible to attacks.

Another major healthcare tech firm - Becton, Dickinson and Company – put out its own warning: “At this time, we are actively monitoring the situation and working closely with customers to ensure the appropriate measures are taken to help safeguard our products.”

Woods said it was likely a wide range of medical systems were taken down by WannaCry. “Many of the bigger machines run the Windows operating system – X-ray, cat scan, MRI,” he said. But, importantly, the parts that actually control the heavy gear that generate the scans aren’t normally controlled by Windows PCs. Many of the pharmacy systems that dispense drugs also run potentially-vulnerable Windows systems, Woods added.

Numerous NHS hospitals are continuing to operate a limited service as of Wednesday. Barts Health Trust, the biggest such trust in the U.K., said it was having to cancel some operations and turn some patients away from the five hospitals it was managing, though some systems were coming back online.

**Industrial control systems hit too**

As for other critical IT infected during the WannaCry pandemic, the U.S.-government funded Industrial Control System Computer Emergency Response Team (ICS-CERT) reported late Tuesday that alongside the healthcare providers, companies including ABB, Rockwell Automation and Schneider Electric had put out their own WannaCry advisories to assist customers.

Robert M. Lee, CEO and founder of the industrial cybersecurity firm Dragos, said his team were “aware of infections that occurred in the industrial control system community and had impact.” Victims included small utilities and manufacturing sites in the U.S., he added, also
pointing to previously-reported infections at Nissan and Renault car manufacturing plants, as well as the attack on Russian Railways.

“Although no one’s been hurt and no safety was at risk.”

Ralph Langner, founder of German control system security consultancy Langner, said that in a typical industrial environment there were “lots of Windows boxes of which a majority is not up to patch.” Attacks on those Windows boxes shouldn’t halt production, however, because industrial machines work autonomously, he added.

But WannaCry has provided ample evidence of vulnerable critical infrastructure. And that’s why Langner’s outlook for the future is grim: “For a competent attacker it would be possible to use the encryption vector specifically against industrial targets and force a production halt. We haven’t seen that on a large scale yet but I predict it’s coming, with ransom demands in the six and seven digits.”

Got a tip? Email at TFox-Brewster@forbes.com or tbthomasbrewster@gmail.com for PGP mail. Get me on Signal on +447837496820 or use SecureDrop to tip anyone at Forbes.
Five nightmarish attacks that show the risks of IoT security

The Internet of Things is not going away -- and neither are the attacks that exploit device vulnerabilities. Here are five incidents that illustrate what users and device developers need to do to prevent breaches.

When it first appeared, the Internet of Things (IoT) seemed to be nothing more than an idea with no substance. What was it? Was it the new ‘IT’ (remember that)? Eventually, IoT came to fruition and consumers lapped it up. Smart thermostats, toasters, locks, lighting, Echo, Google Home... the list goes on and on. As more homes and businesses adopt such devices, you can imagine what follows. Security breaches.
Over the last few years, there have been quite a few IoT-centric attacks. And yet despite the attacks on the rise, IoT continues to enjoy an even greater surge in popularity. Should you consider discontinuing the adoption/deployment of IoT devices -- and forego the convenience of tech evolution?

Let's take a look at some of the worst attacks on IoT devices over the last few years and what you can do to prevent falling victim to vulnerabilities.

1: Stuxnet

I wanted to start off with this particular attack (which occurred between 2010 and 2014), because it perfectly illustrates the inherent danger in IoT devices. Although the devices Stuxnet targeted -- industrial programmable logic controllers (PLCs) -- aren't typical IoT devices per today's standards, they are considered 'smart controllers' and fall into the category. The attack was purportedly launched to sabotage the uranium enrichment facility in Natanz, Iran. Many experts believe that Stuxnet destroyed up to 1,000 centrifuges. Stuxnet was not a typical IoT attack, because it relied on the PLC devices to be connected to a machine running the Windows operating system. Even so, this should have served as a clear warning sign that smart devices can be compromised.

The lesson to be learned from this attack? Mission-critical devices that rely on a standard PC platform should not be attached to a WAN unless absolutely necessary and need to be safeguarded from access by non-critical personnel.

2: Mirai botnet

The year 2016 had plenty of major attacks to call its own. One such attack was the Mirai botnet. This particular botnet infected numerous IoT devices (primarily older routers and IP cameras), then used them to flood DNS provider Dyn with a DDoS attack. The Mirai botnet took down Etsy, GitHub, Netflix, Shopify, SoundCloud, Spotify, Twitter, and a number of other major websites. This piece of malicious code took advantage of devices running out-of-date versions of the Linux kernel and relied on the fact that most users do not change the default usernames/passwords on their devices.

The lesson to be learned from this attack is a bit more complicated than a simple fix. Many companies cut manufacturing costs by not including enough storage space on
their devices to allow for the updating of the Linux kernel. Because of this, a lot of IoT devices are running kernels that include vulnerabilities. It is on the shoulders of the manufacturers to accept this shortcoming and enable every device for regularly scheduled kernel updates. Until this issue is resolved, IoT devices will continue to suffer under the weight of exploits.

It should go without saying that if your IoT device is password protected, you should change the default password (and username, if possible) immediately.

3: Cold in Finland

In November 2016, cybercriminals shut down the heating of two buildings in the city of Lappeenranta, Finland. This was another DDoS attack; in this case, the attack managed to cause the heating controllers to continually reboot the system so that the heating never actually kicked in. Because the temperatures in Finland dip well below freezing at that time of year, this attack was significant.

The lesson learned from this attack? Your network needs to be frequently monitored for DDoS (and other) attacks. The second you see suspect activity on your network... act.

4: Brickerbot
This attack worked in similar fashion to the Mirai botnet, in that it relied upon a DDoS attack and users not changing the default username/password of their device. The biggest difference between Brickerbot (http://www.zdnet.com/article/homeland-security-warns-of-brickerbot-malware-that-destroys-unsecured-internet-connected-devices/) and Mirai botnet is that Brickerbot (as the name implies) simply kills the device. This could be a serious hit on a company’s bottom line if a large deployment of IoT devices are rolled out, only to have them simultaneously bricked.

The lesson learned here is that if your devices include a default username/password, you should immediately change them.

5: The botnet barrage

This year, Verizon Wireless released a report (http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest-2017-sneak-peek_xg_en.pdf) that included an unnamed university that saw more than 5,000 IoT devices attacked. When senior members of the campus IT staff started receiving numerous complaints about slow or inaccessible network connectivity, they discovered their name servers were producing a high volume of alerts and showed an abnormal number of sub-domains related to seafood. It turned out more than 5,000 discrete systems were found to be making hundreds of DNS lookups every 15 minutes. The botnet spread via brute force attack to break through weak passwords on IoT devices.

The lesson learned here? Again, always be on the alert for suspect network activity and make sure to secure your IoT devices with stronger than usual passwords.

Conclusion

From looking at these attacks, it should be clear that the onus for preventing takedown by IoT is on both the user and the device developer. Going forward, every IoT device should ship with an updated kernel/firmware and include the ability to regularly update as new vulnerabilities are found. At the same time, anyone who deploys an IoT device needs to take the time to change the default user/password combination (if available) and constantly be on the lookout for suspect network activity. Finally, developers should seriously consider making default password change a requirement upon initial deployment of the device.

The Internet of Things is not going away. Neither are the attacks on such devices. With just a bit of care during setup and a constant watchful eye on your network, you can prevent security breaches by way of IoT devices.