CHAPTER 1: TANGIBLES

A. Trespass and Nuisance

1. Real Property

RESTATEMENT (SECOND) OF TORTS [TRESPASS TO LAND]

§ 158—*Liability for Intentional Intrusions on Land*

One is subject to liability to another for trespass, irrespective of whether he thereby causes harm to any legally protected interest of the other, if he intentionally

(a) enters land in the possession of the other, or causes a thing or a third person to do so, or

(b) remains on the land, or

(c) fails to remove from the land a thing which he is under a duty to remove.

RESTATEMENT (SECOND) OF TORTS [NUISANCE]

§ 821D—*Private Nuisance*

A private nuisance is a nontrespassory invasion of another's interest in the private use and enjoyment of land.

§ 821F—*Significant Harm*

There is liability for a nuisance only to those to whom it causes significant harm, of a kind that would be suffered by a normal person in the community or by property in normal condition and used for a normal purpose.

§ 826—*Unreasonableness of Intentional Invasion*

An intentional invasion of another's interest in the use and enjoyment of land is unreasonable if

(a) the gravity of the harm outweighs the utility of the actor's conduct, or

(b) the harm caused by the conduct is serious and the financial burden of compensating for this and similar harm to others would not make the continuation of the conduct not feasible.

§ 827—*Gravity of Harm—Factors Involved*

In determining the gravity of the harm from an intentional invasion of another's interest in the use and enjoyment of land, the following factors are important:

(a) The extent of the harm involved;

(b) the character of the harm involved;

(c) the social value that the law attaches to the type of use or enjoyment invaded;

(d) the suitability of the particular use or enjoyment invaded to the character of the locality; and

(e) the burden on the person harmed of avoiding the harm.

§ 829—Gravity vs. Utility—Conduct Malicious or Indecent

An intentional invasion of another's interest in the use and enjoyment of land is unreasonable if the harm is significant and the actor's conduct is

(a) for the sole purpose of causing harm to the other; or

(b) contrary to common standards of decency.

INTERNATIONAL UNION OF PAINTERS AND ALLIED TRADES DISTRICT COUNCIL 15 LOCAL 159 V. GREAT WASH PARK, LLC

No. 67453 (Nev. Ct. App. Aug. 18, 2016)

Before Gibbons, C.J., Silver, J. ...

Members of Local 159 stood on a public sidewalk on Alta Drive and projected a message onto the façade of a building on GWP's property on several occasions. The message noted health code violations of a restaurant on the property. It is undisputed that the image did not cause any physical damage to GWP's property; GWP's claim of irreparable harm arises from the restaurant's lease agreement, which requires the restaurant to pay GWP a percentage of its sales as a portion of its base rent. ...

The Nevada Supreme Court has not issued an opinion on whether light intentionally projected onto private property invades a property right, such that it can constitute a trespass. And there is no statute for civil trespass in Nevada. Our review of trespass law in other jurisdictions reveals two lines of cases. Jurisdictions that adhere to the traditional rule of trespass hold a trespass only occurs "where the invasion of land occurs through a physical, tangible object." *See Babb v. Lee Cty. Landfill SC, LLC*, 747 S.E.2d 468 (S.C. 2013). Jurisdictions that adhere to the modern theory hold that a trespass may also occur when intangible matter, such as particles emanating from a manufacturing plant, cause actual and/or substantial damage to the res. *See Pub. Serv. Co. of Colo. v. Van Wyk*, 27 P.3d 377 (Colo. 2001).

We need not address which theory Nevada should follow because Local 159 did not commit trespass using either theory. Jurisdictions that adhere to either doctrine have stated that light is intangible. Because light is intangible, Local 159 did not commit trespass under the traditional theory. And because the light did not cause damage to GWP's building, Local 159 did not commit trespass under the modern theory. ...

Here, the district court enjoined Local 159's activities on the basis that its "unauthorized and tortious use of GWP's façade constituted an invasion of GWP's property." Because we conclude Local 159's actions cannot constitute a trespass, the district court abused its discretion in issuing the injunction.

Tao, J., concurring:

I join in the court's order of reversal, but as this case involves a protest tactic (using a light projector to beam a message onto a property wall) that may be adopted or copied by other groups or organizations in other circumstances, and in relation to which no Nevada precedent exists, I write to add some further thoughts on the reasons for reversal.

I ...

Virtually all of the "light trespass" cases cited by the parties, and in the court's order, concern the potential trespassory effects of "ambient" light, by which I mean light intended to serve a legitimate ulterior purpose on a nearby property but which incidentally happens to leak or diffuse onto the claimant's property; com-

mon examples of this include construction lighting or light reflecting off the screen of a drive-in movie theater. *See* A*mphitheaters, Inc. v. Portland Meadows*, 198 P.2d 847 (Or. 1948) (ambient light from a drive-in movie theater).

In contrast, this case involves something arguably different: a beam of light specifically and intentionally directed at the Respondents' property and nowhere else that served no purpose other than to intentionally light up the Respondents' building the way the Union wanted. ...

To analogize to a conventional trespass, a trespass committed by a person walking onto prohibited land would be no less a trespass if that person also happened to invade other nearby properties as well during his travels. Similarly, a pedestrian's physical presence on the land constitutes a trespass regardless of whether he was there as part of an exercise routine utterly lacking a message, or whether he was there to make a point about something. Whether that person also trespassed onto other properties along the way, and whether his trespass was with, or free of, communicative purpose, are fundamentally irrelevant to whether a trespass occurred.

And that's the fundamental difference between an invasion by ambient lighting or focused lighting: whether the lighting went into many different directions and lit other properties in addition to this one with no communicative purpose, or whether it went only in one direction and lit only this property to convey a message. ...

IV ...

The torts of trespass and nuisance are closely related, so much so that some courts have observed that expanding the tort of trespass to cover such things as light, gas, or odors effectively blurs the two torts together and makes them one. *See Adams v. Cleveland-Cliffs Iron Co.*, 602 N.W.2d 215 (Mich. App. 1999).

The traditional common-law view was that property injury caused by such things as light, gas, sound, smoke, odors, or vibrations might constitute an actionable nuisance under the right circumstances, but could not support a cause of action in trespass. ...

I agree with the view that light invasions—at least of the kind at issue here—are better suited to be addressed by the law of nuisance than the law of trespass. The fundamental conceptual difference between a trespass and a nuisance is that trespass is the right to exclude something absolutely, while nuisance is the right to exclude something that might have to be tolerated in small quantities but may become the subject of judicial relief when it becomes excessive and unreasonable even in an urban environment.

Thus, the tort of nuisance involves a balancing of competing interests with an eye toward ascertaining the reasonableness of the intrusion, while the tort of trespass is absolute and involves no such balancing. What this means for this case is that, by claiming a trespass to have occurred, the Respondents are seeking an absolute bar against the invasion of projected light, without any inquiry whatsoever into whether the intensity, duration, or other qualities of the projection were unreasonable or excessive. ...

V

Human beings see things only when light is either projected by, or reflects off of, an object and enters the retina; without light, nothing is visible and the world would be dark. Thus, a property such as the Respondent's building can only be seen at all if some source emits enough light to reflect off of the building with suf-

ficient intensity to trigger the nerves within the eye of a human observer. During the daytime, this source can be natural rather than artificial (the sun), but, at night, artificially created and projected light (that is, excluding light from the sun, the moon, and the stars) might be necessary to light the building or else it might be invisible.

Every property located in a densely populated urban area like Las Vegas is continually bombarded by multiple artificial light sources, including such assorted things as street lamps, commercial neon signs, neighboring porch lights, automobile headlights, helicopter searchlights, the ambient glow cast by the Las Vegas Strip over the horizon, and the like, even such barely visible things as pedestrian cell phone screens or cigarette embers. Everything that a human being can see from the property is, technically speaking, a light wave crossing the property line and invading the property.

All of these lights affect the appearance of the property with varying intensity and duration, some brief and barely perceptible, and some with great intensity for long periods of time. If the Respondents are correct and neither intensity nor duration are relevant to whether a trespass has occurred, then all can be the subject of judicial relief no matter how transient or barely perceptible the effect on a property. If the Respondents' argument is correct, then a court could enjoin every light visible from the property anywhere in the city—could order it all turned off—under the rubric of protecting a property right.

Ultimately, when the question is properly framed, the answer strikes me as quite simple: I do not think that the absolute right to block artificial light emanating from somewhere off of the property—without any inquiry into its intensity, duration, reasonableness or unreasonableness—should be included within the "bundle of rights" that one acquires when purchasing a parcel of land in a densely populated urban center like Las Vegas, Trespass law does not convey the right to live in a black hole. I would therefore conclude that the light that was projected in this case does not constitute a violation of the law of trespass. The injunction below was based upon the wrong tort.

On the other hand, simply because a property owner does not have the right to exclude all light emanating onto a property under trespass law does not mean that one must tolerate every kind of light that is beamed onto the property no matter how excessive or unreasonable it may be. In some cases, projecting artificial light onto someone else's property might constitute an actionable private nuisance. The district court's order contains no factual findings regarding whether such a nuisance occurred in this case, and so that question is not before us. ...

WESTCHESTER ASSOCIATES, INC. V. BOSTON EDISON CO.

47 Mass. App. Ct. 133

Jacobs, J.

Westchester Associates, Inc., is the owner of a six-story office building in Framingham immediately adjacent to electric power lines operated by Boston Edison Company. Magnetic fields generated by the power lines have caused disruption and distorted images on computer monitor screens used by tenants who leased space in Westchester's building. ....

Acting under authority of the Department of Public Utilities, Edison, in 1956, took by eminent domain a one-hundred-foot wide easement for the construction and use of one or more transmission lines across land owned by Westchester's predecessor in title. Subsequently two lines were constructed: one carrying 69 kilo-

volts in 1957 and, in 1962, a second line of 13.8 kv. In 1971, a 115 kv line was added, replacing the 1957 line. In 1978, Westchester purchased the land, a portion of which is subject to the easement. It constructed two buildings on the land, one in 1977–1978, and the other, at issue in this case, in 1987. An exterior wall of the 1987 building is located about two feet south of the southern boundary of the easement and about twenty-four feet from the nearest transmission line. Beginning in 1994 when most of the space was leased, tenants soon experienced distorted and "jittery" images on computer screens and the cause was attributed, in the affidavit of an expert, to the magnetic fields generated by Edison's power lines.[5] ...

Discussion. ... Westchester's claim that the fields constitute a nuisance has no legal support. Not only has the character of the magnetic fields generated not changed during the times here relevant, but our law has not recognized those fields as a nuisance.

A significant difficulty with Westchester's attempt to characterize the magnetic fields as a nuisance is that their adverse effects would be experienced only by particular users of equipment sensitive to the fields. There is no contention that the fields are directly detectible by human senses. Thus, they do not constitute an annoyance to a plaintiff of ordinary sensibility. The inquiry to determine whether such fields constitute a nuisance will likely vary as computers and other electronic equipment may become more sophisticated and sensitive. There may come a time when increasing knowledge or changing uses may require, as matter of public policy, the modification of the use of electric power line easements, but this case does not call for such remediation. We conclude that Westchester's nuisance claim, unsupported in the law, fails, and that because Edison reasonably is exercising its easement rights, it is entitled to summary judgment.

NOTES

1. Another union light-projection case involving a union protest, *Urban Philadelphia Liberty Trust v. Center City Organized for Responsible Development,* Nos. 171002675, 3686 EDA 2017 (Ct. Comm. Pleas Penn. Dec. 28, 2017), considered and rejected a nuisance theory. The court explained,

> Photographs taken by both Plaintiff and Defendants confirm that Defendants were careful to project these images onto blank or unused portions of the Hotel's façade rather than into any Hotel rooms or on Plaintiff's signage. ... The mere display of images on the Hotel's facade did not rise to the level of significant harm required for a nuisance. Indeed, public protests typically involve activity or expressive conduct that is designed to

5. Westchester's expert concludes that the magnetic fields generated by the power lines caused the "jittery" images by disrupting the magnetic field generated internally by those devices which serves to direct and focus the images on the screens. He states that the resulting movement of the images on the screens is "most unpleasant to watch for any length of time whatsoever." He also notes that, because magnetic fields from power lines are "present in most environments," manufacturers of video screens provide shielding to protect them from interference that is effective for field strengths of "a few milliGauss." He opines that, in the range of ten milliGauss and above, such shielding is not effective. Actual measurements made in the building by an expert for one of the tenants generally were well above that value in the office areas located along the wall of Westchester's building nearest to Edison's lines.

call attention to the protestors' message, which is the very essence of the First Amendment.

2. For an argument that courts should sometimes allow landowners to sue to prevent targeted projections because there is an interest in "protecting an owner's communicative interests against intentional interference", see Maureen E. Brady, *Property and Projection*, 133 HARV. L. REV. 1143 (2020).

2. Personal Property

RESTATEMENT (SECOND) OF TORTS [CONVERSION]

§ 222A—*What Constitutes Conversion*

(1) Conversion is an intentional exercise of dominion or control over a chattel which so seriously interferes with the right of another to control it that the actor may justly be required to pay the other the full value of the chattel. ...

§ 226—*Conversion by Destruction or Alteration*

One who intentionally destroys a chattel or so materially alters its physical condition as to change its identity or character is subject to liability for conversion to another who is in possession of the chattel or entitled to its immediate possession.

§ 226—*Conversion by Using Chattel*

One who uses a chattel in a manner which is a serious violation of the right of another to control its use is subject to liability to the other for conversion.

§ 228—*Exceeding Authorized Use*

One who is authorized to make a particular use of a chattel, and uses it in a manner exceeding the authorization, is subject to liability for conversion to another whose right to control the use of the chattel is thereby seriously violated.

RESTATEMENT (SECOND) OF TORTS [TRESPASS TO CHATTELS]

§ 218—*Liability to Person in Possession*

One who commits a trespass to a chattel is subject to liability to the possessor of the chattel if, but only if,

(a) he dispossesses the other of the chattel, or

(b) the chattel is impaired as to its condition, quality, or value, or

(c) the possessor is deprived of the use of the chattel for a substantial time, or

(d) bodily harm is caused to the possessor, or harm is caused to some person or thing in which the possessor has a legally protected interest.

Comment on Clauses (b) and (c):

e. The interest of a possessor of a chattel in its inviolability, unlike the similar interest of a possessor of land, is not given legal protection by an action for nominal damages for harmless intermeddlings with the chattel. In order that an actor who interferes with another's chattel may be liable, his conduct must affect some other and more important interest of the possessor. Therefore, one who intentionally intermeddles with another's chattel is subject to liability only if his intermeddling is harmful to the possessor's materially valuable interest in the physical condition, quality, or value of the chattel, or if the possessor is deprived of the use of the chattel for a substantial time, or some other legally protected interest of the possessor is affected as stated in Clause (c). Sufficient legal protection of the possessor's in-

terest in the mere inviolability of his chattel is afforded by his privilege to use reasonable force to protect his possession against even harmless interference.

Illustration:

2. A, a child, climbs upon the back of B's large dog and pulls its ears. No harm is done to the dog, or to any other legally protected interest of B. A is not liable to B.

IN RE STARLINK CORN PRODUCTS LIABILITY LITIGATION

212 F.Supp.2d 828 (N.D. Ill. 2002)

Moran, Senior District Judge: ...

BACKGROUND

Aventis genetically engineered a corn seed to produce a protein known as Cry9C that is toxic to certain insects. The seeds are marketed under the brand name StarLink. Garst is a licensee who produced and distributed StarLink seeds. Aventis applied to register StarLink with the EPA, which is responsible for regulating insecticides under the [Federal Insecticide, Fungicide and Rodenticide Act], 7 U.S.C. §§ 136 *et seq*. The EPA noted that Cry9C had several attributes similar to known human allergens, and issued only a limited registration, permitting StarLink use for such purposes as animal feed, ethanol production and seed increase, but prohibiting its use for human consumption.

[The EPA required special procedures for StarLink corn, including segregating it from other corn and instructing farmers on how to handle it. The plaintiffs alleged that Aventis failed to comply with these procedures, and that as a result the U.S. corn supply became widely contaminated with StarLink corn.]

Fear of StarLink contamination nonetheless continues to affect corn markets. Many U.S. food producers have stopped using U.S. corn, replacing it with imported corn or corn substitutes. South Korea, Japan and other foreign countries have terminated or substantially limited imports of U.S. corn. Grain elevators and transport providers are now mandating expensive testing on all corn shipments. ...

IV. CONVERSION

Conversion is defined as "an intentional exercise of dominion or control over a chattel which so seriously interferes with the right of another to control it that the actor may justly be required to pay the other the full value of the chattel." Restatement (Second) of Torts § 222A. Plaintiffs argue that defendants' role in contaminating the corn supply amounts to a conversion of their property. We disagree.

The defining element of conversion, the one that distinguishes it from a trespass to chattels, is the extent of interference with the owner's property rights. If the damage is minor, in duration or severity, plaintiff may only recover for the diminished value. But if the damage is sufficiently severe, plaintiff may recover full value. Conversion is akin to a forced judicial sale. The defendant pays full value for the chattel, and receives title to it. Restatement § 222A comment c. Here, plaintiffs have not alleged that defendants destroyed their crops or deprived them of possession. Plaintiffs retained possession and still had total control over the corn. Most, if not all of it, was ultimately sold to third parties. The only damages were a lower price, for which plaintiffs could be compensated without forcing a sale.

It is possible to convert a chattel by altering it, without completely destroying it. In particular, commingling fungible goods so that their identity is lost can constitute a conversion. Restatement § 226 comment e. To do so, however, the perpetrator must alter the chattel in a way that is "so material as to change the identity

of the chattel or its essential character." Restatement § 226 comment d. At worst, StarLink contamination changed plaintiffs' yield from being corn fit for human consumption to corn fit only for domestic or industrial use. Plaintiffs do not claim they were growing the corn to eat themselves, but for sale on the commodity markets. The crops were still viable for the purpose for which plaintiffs would normally use them, for sale on the open market. That the market had become less hospitable does not change the product's essential character. As above, the severity of the alteration is indicated by the decrease in market price. This could arguably constitute a trespass to chattels, but does not rise to the level of conversion.

Lastly, negligence cannot support a conversion claim. It requires intent. Restatement § 224. The complaint alleges that defendants did not take adequate precautions to ensure that StarLink corn was adequately segregated. Nowhere do plaintiffs claim that defendants intentionally commingled StarLink and non-StarLink corn, or deliberately contaminated the food supply. Even if defendants negligently failed to prevent cross-pollination and commingling, they would not be liable for conversion.

B. Online Trespass

1. Trespass to Chattels

INTEL V. HAMIDI
71 P. 3d 296 (Cal. 2003)

Werdegar, Justice: ...

[Kourosh Kenneth] Hamidi, a former Intel engineer, together with others, formed an organization named Former and Current Employees of Intel (FACE-Intel) to disseminate information and views critical of Intel's employment and personnel policies and practices. FACE-Intel maintained a Web site (which identified Hamidi as Webmaster and as the organization's spokesperson) containing such material. In addition, over a 21-month period Hamidi, on behalf of FACE-Intel, sent six mass e-mails to employee addresses on Intel's electronic mail system. The messages criticized Intel's employment practices, warned employees of the dangers those practices posed to their careers, suggested employees consider moving to other companies, solicited employees' participation in FACE-Intel, and urged employees to inform themselves further by visiting FACE-Intel's Web site. The messages stated that recipients could, by notifying the sender of their wishes, be removed from FACE-Intel's mailing list; Hamidi did not subsequently send messages to anyone who requested removal.

Each message was sent to thousands of addresses (as many as 35,000 according to FACE-Intel's Web site), though some messages were blocked by Intel before reaching employees. Intel's attempt to block internal transmission of the messages succeeded only in part; Hamidi later admitted he evaded blocking efforts by using different sending computers. When Intel, in March 1998, demanded in writing that Hamidi and FACE-Intel stop sending e-mails to Intel's computer system, Hamidi asserted the organization had a right to communicate with willing Intel employees; he sent a new mass mailing in September 1998.

The summary judgment record contains no evidence Hamidi breached Intel's computer security in order to obtain the recipient addresses for his messages; in-

deed, internal Intel memoranda show the company's management concluded no security breach had occurred. Hamidi stated he created the recipient address list using an Intel directory on a floppy disk anonymously sent to him. Nor is there any evidence that the receipt or internal distribution of Hamidi's electronic messages damaged Intel's computer system or slowed or impaired its functioning. Intel did present uncontradicted evidence, however, that many employee recipients asked a company official to stop the messages and that staff time was consumed in attempts to block further messages from FACE-Intel. According to the FAC-Intel Web site, moreover, the messages had prompted discussions between "[e]xcited and nervous managers" and the company's human resources department.

Intel sued Hamidi and FACE-Intel [for trespass to chattels] and seeking both actual damages and an injunction against further e-mail messages. [The trial court granted Intel's motion for summary judgment and enjoined Hamidi from any further mailings. A divided Court of Appeal affirmed.]

I. CURRENT CALIFORNIA TORT LAW

Dubbed by Prosser the "little brother of conversion," the tort of trespass to chattels allows recovery for interferences with possession of personal property "not sufficiently important to be classed as conversion, and so to compel the defendant to pay the full value of the thing with which he has interfered." PROSSER & KEETON, TORTS § 14 (5th ed. 1984).

Though not amounting to conversion, the defendant's interference must, to be actionable, have caused some injury to the chattel or to the plaintiffs rights in it. ...

The Restatement, too, makes clear that some actual injury must have occurred in order for a trespass to chattels to be actionable. Under section 218 of the Restatement Second of Torts, dispossession alone, without further damages, is actionable, but other forms of interference require some additional harm to the personal property or the possessor's interests in it.

> The interest of a possessor of a chattel in its inviolability, unlike the similar interest of a possessor of land, is not given legal protection by an action for nominal damages for harmless intermeddlings with the chattel. In order that an actor who interferes with another's chattel may be liable, his conduct must affect some other and more important interest of the possessor. Therefore, one who intentionally intermeddles with another's chattel is subject to liability only if his intermeddling is harmful to the possessor's materially valuable interest in the physical condition, quality, or value of the chattel, or if the possessor is deprived of the use of the chattel for a substantial time, or some other legally protected interest of the possessor is affected as stated in Clause (c). Sufficient legal protection of the possessor's interest in the mere inviolability of his chattel is afforded by his privilege to use reasonable force to protect his possession against even harmless interference.

Intel suggests that the requirement of actual harm does not apply here because it sought only injunctive relief, as protection from future injuries. But as Justice Kolkey, dissenting below, observed, "[t]he fact the relief sought is injunctive does not excuse a showing of injury, whether actual or threatened." Indeed, in order to obtain injunctive relief the plaintiff must ordinarily show that the defendant's wrongful acts threaten to cause irreparable injuries, ones that cannot be adequately compensated in damages. ...

The dispositive issue in this case, therefore, is whether the undisputed facts demonstrate Hamidi's actions caused or threatened to cause damage to Intel's computer system, or injury to its rights in that personal property, such as to entitle Intel to judgment as a matter of law. To review, the undisputed evidence revealed no actual or threatened damage to Intel's computer hardware or software and no interference with its ordinary and intended operation. Intel was not dispossessed of its computers, nor did Hamidi's messages prevent Intel from using its computers for any measurable length of time. Intel presented no evidence its system was slowed or otherwise impaired by the burden of delivering Hamidi's electronic messages. Nor was there any evidence transmission of the messages imposed any marginal cost on the operation of Intel's computers. In sum, no evidence suggested that in sending messages through Intel's Internet connections and internal computer system Hamidi used the system in any manner in which it was not intended to function or impaired the system in any way. Nor does the evidence show the request of any employee to be removed from FACE-Intel's mailing list was not honored. The evidence did show, however, that some employees who found the messages unwelcome asked management to stop them and that Intel technical staff spent time and effort attempting to block the messages. A statement on the FACE-Intel Web site, moreover, could be taken as an admission that the messages had caused "[e]xcited and nervous managers" to discuss the matter with Intel's human resources department.

Relying on a line of decisions, most from federal district courts, applying the tort of trespass to chattels to various types of unwanted electronic contact between computers, Intel contends that, while its computers were not damaged by receiving Hamidi's messages, its interest in the "physical condition, quality or value," RESTATEMENT (SECOND) OF TORTS § 218 cmt. e, of the computers was harmed. We disagree. The cited line of decisions does not persuade us that the mere sending of electronic communications that assertedly cause injury only because of their contents constitutes an actionable trespass to a computer system through which the messages are transmitted. Rather, the decisions finding electronic contact to be a trespass to computer systems have generally involved some actual or threatened interference with the computers' functioning.

In *Thrifty-Tel, Inc. v. Bezenek*, 46 Cal. App. 4th 1559 (1996), the California Court of Appeal held that evidence of automated searching of a telephone carrier's system for authorization codes supported a cause of action for trespass to chattels. The defendant's automated dialing program "overburdened the [plaintiffs] system, denying some subscribers access to phone lines," showing the requisite injury.

Following *Thrifty-Tel*, a series of federal district court decisions held that sending UCE through an ISP's equipment may constitute trespass to the ISP's computer system. The lead case, *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015 (S.D. Ohio 1997), was followed by *Hotmail Corp. v. Van$ Money Pie, Inc.*, No. C 98-20064 JW, 1998 WL 388389 (N.D. Cal., Apr. 16, 1998), *America Online, Inc. v. IMS*, 24 F. Supp. 2d 548, (E.D. Va. 1998), and *America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444 (E.D. Va. 1998).

In each of these spamming cases, the plaintiff showed, or was prepared to show, some interference with the efficient functioning of its computer system. In *CompuServe*, the plaintiff ISP's mail equipment monitor stated that mass UCE mailings, especially from nonexistent addresses such as those used by the defendant, placed "a tremendous burden" on the ISP's equipment, using "disk space and draining] the processing power," making those resources unavailable to serve sub-

scribers. Similarly, in *Hotmail Corp. v. Van$ Money Pie, Inc.*, the court found the evidence supported a finding that the defendant's mailings "fill[ed] up Hotmail's computer storage space and threatened to damage Hotmail's ability to service its legitimate customers." ...

In the leading case, *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058 (N.D. Cal. 2000), the defendant Bidder's Edge (BE), operating an auction aggregation site, accessed the eBay Web site about 100,000 times per day, accounting for between 1 and 2 percent of the information requests received by eBay and a slightly smaller percentage of the data transferred by eBay. The district court rejected eBay's claim that it was entitled to injunctive relief because of the defendant's unauthorized presence alone, or because of the incremental cost the defendant had imposed on operation of the eBay site, but found sufficient proof of *threatened* harm in the potential for others to imitate the defendant's activity: "If BE's activity is allowed to continue unchecked, it would encourage other auction aggregators to engage in similar recursive searching of the eBay system such that eBay would suffer irreparable harm from reduced system performance, system unavailability, or data losses." *Id.* at 1066. Again, in addressing the likelihood of eBay's success on its trespass to chattels cause of action, the court held the evidence of injury to eBay's computer system sufficient to support a preliminary injunction: "If the court were to hold otherwise, it would likely encourage other auction aggregators to crawl the eBay site, potentially to the point of denying effective access to eBay's customers. If preliminary injunctive relief were denied, and other aggregators began to crawl the eBay site, there appears to be little doubt that the load on eBay's computer system would qualify as a substantial impairment of condition or value." *Id.* at 1071-1072. ...

That Intel does not claim the type of functional impact that spammers and robots have been alleged to cause is not surprising in light of the differences between Hamidi's activities and those of a commercial enterprise that uses sheer quantity of messages as its communications strategy. Though Hamidi sent thousands of copies of the same message on six occasions over 21 months, that number is minuscule compared to the amounts of mail sent by commercial operations. The individual advertisers sued in *America Online, Inc. v. IMS* and *America Online, Inc. v. LCGM, Inc.* were alleged to have sent more than 60 million messages over 10 months and more than 92 million messages over seven months, respectively. Collectively, UCE has reportedly come to constitute about 45 percent of all e-mail. The functional burden on Intel's computers, or the cost in time to individual recipients, of receiving Hamidi's occasional advocacy messages cannot be compared to the burdens and costs caused ISP's and their customers by the ever-rising deluge of commercial e-mail.

Intel relies on language in the eBay decision suggesting that unauthorized use of another's chattel is actionable even without any showing of injury: "Even if, as [defendant] BE argues, its searches use only a small amount of eBay's computer system capacity, BE has nonetheless deprived eBay of the ability to use that portion of its personal property for its own purposes. The law recognizes no such right to use another's personal property." *eBay*, 100 F. Supp. 2d at. 1071. But as the *eBay* court went on immediately to find that the defendant's conduct, if widely replicated, would likely impair the functioning of the plaintiffs system, we do not read the quoted remarks as expressing the court's complete view of the issue. In isolation, moreover, they would not be a correct statement of California or general American law on this point. While one may have no right temporarily to use another's per-

sonal property, such use is actionable as a trespass only if it "has proximately caused injury." *Thrifty-Tel*, 46 Cal. App. 4th at 1566. ... That Hamidi's messages temporarily used some portion of the Intel computers' processors or storage is, therefore, not enough; Intel must, but does not, demonstrate some measurable loss from the use of its computer system. ...

This theory of "impairment by content," Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 1 (1999), threatens to stretch trespass law to cover injuries far afield from the harms to possession the tort evolved to protect. Intel's theory would expand the tort of trespass to chattels to cover virtually any unconsented-to communication that, solely because of its content, is unwelcome to the recipient or intermediate transmitter. As the dissenting justice below explained

> "Damage" of this nature—the distraction of reading or listening to an unsolicited communication—is not within the scope of the injury against which the trespass-to-chattel tort protects, and indeed trivializes it. After all, "[t]he property interest protected by the old action of trespass was that of possession; and this has continued to affect the character of the action." PROSSER & KEETON § 14. Reading an e-mail transmitted to equipment designed to receive it, in and of itself, does not affect the possessory interest in the equipment. Indeed, if a chattel's receipt of an electronic communication constitutes a trespass to that chattel, then not only are unsolicited telephone calls and faxes trespasses to chattel, but unwelcome radio waves and television signals also constitute a trespass to chattel every time the viewer inadvertently sees or hears the unwanted program.

We agree. While unwelcome communications, electronic or otherwise, can cause a variety of injuries to economic relations, reputation and emotions, those interests are protected by other branches of tort law; in order to address them, we need not create a fiction of injury to the communication system.

Nor may Intel appropriately assert a property interest in its employees' time. "The Restatement test clearly speaks in the first instance to the impairment of the chattel.... But employees are not chattels (at least not in the legal sense of the term)." Burk, *The Trouble with Trespass*, at 36. Whatever interest Intel may have in preventing its employees from receiving disruptive communications, it is not an interest in personal property, and trespass to chattels is therefore not an action that will lie to protect it. Nor, finally, can the fact Intel staff spent time attempting to block Hamidi's messages be bootstrapped into an injury to Intel's possessory interest in its computers. To quote, again, from the dissenting opinion in the Court of Appeal: "[I]t is circular to premise the damage element of a tort solely upon the steps taken to prevent the damage. Injury can only be established by the completed tort's consequences, not by the cost of the steps taken to avoid the injury and prevent the tort; otherwise, we can create injury for every supposed tort."

Intel connected its e-mail system to the Internet and permitted its employees to make use of this connection both for business and, to a reasonable extent, for their own purposes. In doing so, the company necessarily contemplated the employees' receipt of unsolicited as well as solicited communications from other companies and individuals. That some communications would, because of their contents, be unwelcome to Intel management was virtually inevitable. Hamidi did nothing but use the e-mail system for its intended purpose—to communicate with employees. The system worked as designed, delivering the messages without any physical or functional harm or disruption. These occasional transmissions cannot reasonably

be viewed as impairing the quality or value of Intel's computer system. We conclude, therefore, that Intel has not presented undisputed facts demonstrating an injury to its personal property, or to its legal interest in that property, that support, under California tort law, an action for trespass to chattels.

II. Proposed Extension of California Tort Law

We next consider whether California common law should be *extended* to cover, as a trespass to chattels, an otherwise harmless electronic communication whose contents are objectionable. We decline to so expand California law. Intel, of course, was not the recipient of Hamidi's messages, but rather the owner and possessor of computer servers used to relay the messages, and it bases this tort action on that ownership and possession. The property rule proposed is a rigid one, under which the sender of an electronic message would be strictly liable to the owner of equipment through which the communication passes—here, Intel—for any consequential injury flowing from the *contents* of the communication. The arguments of amici curiae and academic writers on this topic, discussed below, leave us highly doubtful whether creation of such a rigid property rule would be wise.

Writing on behalf of several industry groups appearing as amici curiae, Professor Richard A. Epstein of the University of Chicago urges us to excuse the required showing of injury to personal property in cases of unauthorized electronic contact between computers, "extending the rules of trespass to real property to all interactive Web sites and servers." The court is thus urged to recognize, for owners of a particular species of personal property, computer servers, the same interest in inviolability as is generally accorded a possessor of land. In effect, Professor Epstein suggests that a company's server should be its castle, upon which any unauthorized intrusion, however harmless, is a trespass.

Epstein's argument derives, in part, from the familiar metaphor of the Internet as a physical space, reflected in much of the language that has been used to describe it: "cyberspace," "the information superhighway," e-mail "addresses," and the like. Of course, the Internet is also frequently called simply the "Net," a term, Hamidi points out, "evoking a fisherman's chattel." A major component of the Internet is the World Wide "Web," a descriptive term suggesting neither personal nor real property, and "cyberspace" itself has come to be known by the oxymoronic phrase "virtual reality," which would suggest that any real property "located" in "cyberspace" must be "virtually real" property. Metaphor is a two-edged sword.

Indeed, the metaphorical application of real property rules would not, by itself, transform a physically harmless electronic intrusion on a computer server into a trespass. That is because, under California law, intangible intrusions on land, including electromagnetic transmissions, are not actionable as trespasses (though they may be as nuisances) unless they cause physical damage to the real property. Since Intel does not claim Hamidi's electronically transmitted messages physically damaged its servers, it could not prove a trespass to land even were we to treat the computers as a type of real property. Some further extension of the conceit would be required, under which the electronic signals Hamidi sent would be recast as tangible intruders, perhaps as tiny messengers rushing through the "hallways" of Intel's computers and bursting out of employees' computers to read them Hamidi's missives. But such fictions promise more confusion than clarity in the law. *See eBay v. Bidder's Edge*, 100 F. Supp. 2d 1058, 1065–66 (rejecting eBay's argument that the defendant's automated data searches "should be thought of as equivalent to sending in an army of 100,000 robots a day to check the prices in a competitor's store").

The plain fact is that computers, even those making up the Internet, are—like such older communications equipment as telephones and fax machines—personal property, not realty. Professor Epstein observes that "athough servers may be moved in real space, they cannot be moved in cyberspace," because an Internet server must, to be useful, be accessible at a known address. But the same is true of the telephone: to be useful for incoming communication, the telephone must remain constantly linked to the same number (or, when the number is changed, the system must include some forwarding or notification capability, a qualification that also applies to computer addresses). Does this suggest that an unwelcome message delivered through a telephone or fax machine should be viewed as a trespass to a type of real property? We think not: As already discussed, the contents of a telephone communication may cause a variety of injuries and may be the basis for a variety of tort actions (e.g., defamation, intentional infliction of emotional distress, invasion of privacy), but the injuries are not to an interest in property, much less real property, and the appropriate tort is not trespass.

More substantively, Professor Epstein argues that a rule of computer server inviolability will, through the formation or extension of a market in computer-to-computer access, create "the right social result," In most circumstances, he predicts, companies with computers on the Internet will continue to authorize transmission of information through e-mail, Web site searching, and page linking because they benefit by that open access. When a Web site owner does deny access to a particular sending, searching, or linking computer, a system of "simple one-on-one negotiations" will arise to provide the necessary individual licenses.

Other scholars are less optimistic about such a complete propertization of the Internet. Professor Mark Lemley of the University of California, Berkeley, writing on behalf of an amici curiae group of professors of intellectual property and computer law, observes that under a property rule of server inviolability, "each of the hundreds of millions of Internet users must get permission in advance from anyone with whom they want to communicate and anyone who owns a server through which their message may travel." The consequence for e-mail could be a substantial reduction in the freedom of electronic communication, as the owner of each computer through which an electronic message passes could impose its own limitations on message content or source. As Professor Dan Hunter of the University of Pennsylvania asks rhetorically: "Does this mean that one must read the 'Terms of Acceptable Email Usage' of every email system that one emails in the course of an ordinary day? If the University of Pennsylvania had a policy that sending a joke by email would be an unauthorized use of their system, then under the logic of [the lower court decision in this case], you commit 'trespass' if you emailed me a cartoon." Daniel Hunter, *Cyberspace as Place, and the Tragedy of the Digital Anticommons,* 91 CAL. L.REV. 439, 508-509 (2003).

Web site linking, Professor Lemley further observes, "would exist at the sufferance of the linked-to party, because a Web user who followed a 'disapproved' link would be trespassing on the plaintiffs server, just as sending an e-mail is trespass under the [lower] court's theory." Another writer warns that "cyber-trespass theory will curtail the free flow of price and product information on the Internet by allowing website owners to tightly control who and what may enter and make use of the information housed on its Internet site." Edward W. Chang, *Bidding on Trespass: eBay, Inc. v. Bidder's Edge, Inc. and the Abuse of Trespass Theory in Cyberspace Law*29 AIPLA Q.J. 445, 459 (2001). A leading scholar of Internet law and policy, Professor Lawrence Lessig of Stanford University, has criticized Professor

Epstein's theory of the computer server as quasi-real property, previously put forward in the *eBay* case, on the ground that it ignores the costs to society in the loss of network benefits: "eBay benefits greatly from a network that is open and where access is free. It is this general feature of the Net that makes the Net so valuable to users and a source of great innovation. And to the extent that individual sites begin to impose their own rules of exclusion, the value of the network as a network declines. If machines must negotiate before entering any individual site, then the costs of using the network climb." Lawrence Lessig, *The Future of Ideas: The Fate of the Commons in a Connected World* 171 (2001) p. 171

We discuss this debate among the amici curiae and academic writers only to note its existence and contours, not to attempt its resolution. Creating an absolute property right to exclude undesired communications from one's e-mail and Web servers might help force spammers to internalize the costs they impose on ISP's and their customers. But such a property rule might also create substantial new costs, to e-mail and e-commerce users and to society generally, in lost ease and openness of communication and in lost network benefits. In light of the unresolved controversy, we would be acting rashly to adopt a rule treating computer servers as real property for purposes of trespass law.

The Legislature has already adopted detailed regulations governing [Unsolicited Commercial Email, i.e. spam.] It may see fit in the future also to regulate noncommercial e-mail, such as that sent by Hamidi, or other kinds of unwanted contact between computers on the Internet, such as that alleged in *eBay*. But we are not persuaded that these perceived problems call at present for judicial creation of a rigid property rule of computer server inviolability. We therefore decline to create an exception, covering Hamidi's unwanted electronic messages to Intel employees, to the general rule that a trespass to chattels is not actionable if it does not involve actual or threatened injury to the personal property or to the possessor's legally protected interest in the personal property. No such injury having been shown on the undisputed facts, Intel was not entitled to summary judgment in its favor. ...

Kennard, Justice, concurring: ...

Intel has my sympathy. Unsolicited and unwanted bulk e-mail, most of it commercial, is a serious annoyance and inconvenience for persons who communicate electronically through the Internet, and bulk e-mail that distracts employees in the workplace can adversely affect overall productivity. But, as the majority persuasively explains, to establish the tort of trespass to chattels in California, the plaintiff must prove either damage to the plaintiff's personal property or actual or threatened impairment of the plaintiff's ability to use that property. Because plaintiff Intel has not shown that defendant Hamidi's occasional bulk e-mail messages to Intel's employees have damaged Intel's computer system or impaired its functioning in any significant way, Intel has not established the tort of trespass to chattels.

This is not to say that Intel is helpless either practically or legally. As a practical matter, Intel need only instruct its employees to delete messages from Hamidi without reading them and to notify Hamidi to remove their workplace e-mail addresses from his mailing lists. Hamidi's messages promised to remove recipients from the mailing list on request, and there is no evidence that Hamidi has ever failed to do so. From a legal perspective, a tort theory other than trespass to chattels may provide Intel with an effective remedy if Hamidi's messages are defamatory or wrongfully interfere with Intel's economic interests. Additionally, the Leg-

islature continues to study the problems caused by bulk e-mails and other dubious uses of modern communication technologies and may craft legislation that accommodates the competing concerns in these sensitive and highly complex areas.

Brown, Justice, dissenting:

Candidate A finds the vehicles that candidate B has provided for his campaign workers, and A spray paints the water soluble message, "Fight corruption, vote for A" on the bumpers. The majority's reasoning would find that notwithstanding the time it takes the workers to remove the paint and the expense they incur in altering the bumpers to prevent further unwanted messages, candidate B does not deserve an injunction unless the paint is so heavy that it reduces the cars' gas mileage or otherwise depreciates the cars' market value. Furthermore, candidate B has an obligation to permit the paint's display, because the cars are driven by workers and not B personally, because B allows his workers to use the cars to pick up their lunch or retrieve their children from school, or because the bumpers display B's own slogans. I disagree.

Intel has invested millions of dollars to develop and maintain a computer system. It did this not to act as a public forum but to enhance the productivity of its employees. Kourosh Kenneth Hamidi sent as many as 200,000 e-mail messages to Intel employees. The time required to review and delete Hamidi's messages diverted employees from productive tasks and undermined the utility of the computer system. "There may . . . be situations in which the value to the owner of a particular type of chattel may be impaired by dealing with it in a manner that does not affect its physical condition." RESTATEMENT (SECOND) OF TORTS § 218 cmt. h. This is such a case.

The majority repeatedly asserts that Intel objected to the hundreds of thousands of messages solely due to their content, and proposes that Intel seek relief by pleading content-based speech torts. This proposal misses the point that Intel's objection is directed not toward Hamidi's message but his use of Intel's property to display his message. Intel has not sought to prevent Hamidi from expressing his ideas on his Web site, through private mail (paper or electronic) to employees' homes, or through any other means like picketing or billboards. But as counsel for Intel explained during oral argument, the company objects to Hamidi's using Intel's property to advance his message.

Of course, Intel deserves an injunction even if its objections are based entirely on the e-mail's content. Intel is entitled, for example, to allow employees use of the Internet to check stock market tables or weather forecasts without incurring any concomitant obligation to allow access to pornographic Web sites. A private property owner may choose to exclude unwanted mail for any reason, including its content. ...

Mosk, Justice, dissenting: ...

The majority fail to distinguish open communication in the public "commons" of the Internet from unauthorized intermeddling on a private, proprietary intranet. Hamidi is not communicating in the equivalent of a town square or of an unsolicited "junk" mailing through the United States Postal Service. His action, in crossing from the public Internet into a private intranet, is more like intruding into a private office mailroom, commandeering the mail cart, and dropping off unwanted broadsides on 30,000 desks. Because Intel's security measures have been circumvented by Hamidi, the majority leave Intel, which has exercised all reasonable self-help efforts, with no recourse unless he causes a malfunction or

systems "crash." Hamidi's repeated intrusions did more than merely "prompt[] discussions between '[e]xcited and nervous managers' and the company's human resource department" (maj. opn., ante); they also constituted a misappropriation of Intel's private computer system contrary to its intended use and against Intel's wishes.

UNIVERSAL TUBE & ROLLFORM EQUIP. CORP. V. YOUTUBE, INC.

504 F. Supp. 2d 260

Carr, Chief Judge: ...

Background

Universal, which has been in the business of supplying used tube and pipe mills and rollform machinery for over two decades, purchased the www.utube.com domain name in 1996. ...

The predecessors of YouTube registered the youtube.com domain name in February, 2005. The company was later incorporated in October, 2005, and its website publicly launched in December, 2005.

Universal claims that the presence of youtube.com has caused several problems. Traffic at utube.com's website increased from a "few thousand" visitors per month before youtube.com began operating to approximately 70,000 visitors per day. This influx of visitors has caused Universal's web servers to crash on multiple occasions. This, in turn, impedes access to Universal's website by its customers, with a resultant loss in sales.

Universal also contends that its internet hosting fees (fees paid to third parties to host the utube.com website on third party computers) increased from less than $100.00 per month to more than $2,500 per month. The unintended visitors have also disrupted Universal's business by leaving inappropriate and harassing messages through the utube.com site. ...

Discussion

3. Trespass to Chattels

Universal claims relief for trespass to chattels. Plaintiff says it" "owns the "chattel " and that YouTube's actions have "diminished the value, quality or condition of the chattel." Universal also alleges that it "hosts its website on certain server computers" and that YouTube has caused those computers to "shut down and crash."

YouTube seeks to dismiss Universal's claim for trespass to chattels on several grounds. First, YouTube claims that Universal has failed to make the necessary allegation that YouTube intentionally came into physical contact with Universal's property. Instead, mistaken internet visitors are the ones who make contact with Universal's website.

Second, YouTube argues that utube.com is a website, and that websites do not meet the definition of chattel. According to YouTube, "chattel" must be movable, physical, personal property, which a website is not.

Universal argues that both the domain name and the webservers that plaintiff leases are the chattels involved in this case. Plaintiff also challenges whether intentionally is an element of trespass to chattel under Ohio law. Plaintiff urges the court to allow the claim to continue so that its "novel claim" can be fleshed out with facts.

Universal also argues that to satisfy the requirements of its claim, the "intermeddling" with its chattel need not be performed by YouTube itself, but instead

could be performed indirectly by third parties, so long as the harm is still attributable to YouTube's use of its domain name.

Even if a domain name does not qualify as chattel, Universal argues in its briefs that it has a "personal property interest" in the computer system that hosts the utube.com website. Universal represents through its briefs that it has a contractual agreement that is "essentially" a "lease for the use of a specific portion of the computer system."

Despite being a well-aged cause of action, trespass to chattels has been applied in the context of the internet. In *Compu-Serve, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1022 (S.D.Ohio 1997), the court held that a "spammer" (sender of unsolicited email) could be held liable to an internet service provider for sending unsolicited emails to the provider's clients. The court found that "electronic signals generated and sent by computer" were "sufficiently physically tangible to support a trespass cause of action." *Id.* at 1021.

What *CompuServe* makes clear is that the focus of a trespass to chattel claim, although it involves something as amorphous as "the internet," must still maintain some link to a physical object—in that case, a computer. *Id.* (discussing necessity of "physical contact" with the chattel); *Restatement (Second) of Torts* 217 cmt. (defining "intermeddling" as "intentionally bringing about a physical contact with the chattel"). A domain name is an intangible object, much like a street address or a telephone number, which, though it may ultimately point to an approximate or precise physical location, is without physical substance, and it is therefore impossible to make "physical contact" with it. Universal's only hope of succeeding on its trespass to chattels claim, therefore, rests on its ability to show a link to a physical object. In this case, the only such physical object is the computer [or computers] hosting Universal's website.

To make a claim for trespass, one must have a possessory interest in the property in question. Universal represented that it entered into a contract with a third party to host the utube.com website on the third party's computers. Universal therefore has not alleged that it has a possessory interest in the host's computers, and no inference can be drawn from its allegations that Universal has a possessory interest.

Universal's claim for trespass to chattels also fails because YouTube did not make physical contact with the computers hosting the website. In CompuServe, the defendant trespasser clearly initiated contact. In this case, those making contact with Universal's website were thousands of mistaken visitors, but not YouTube itself.

Section 217 of the Restatement (Second) of Torts (which is followed in Ohio) discusses indirect physical contact ("intermeddling"):

> "Intermeddling" means intentionally bringing about a physical contact with the chattel. The actor may commit a trespass by an act which brings him into an intended physical contact with a chattel in the possession of another, as when he beats another's horse or dog, or by intentionally directing an object or missile against it, as when the actor throws a stone at another's automobile or intentionally drives his own car against it. So too, *a trespass may be committed by causing a third person through duress or fraud to intermeddle with another's chattel.* (emphasis added)

Presumably, the Restatement creates exceptions for duress and fraud because, in those circumstances, the one making physical contact is deprived of accurate in-

formation or free will and becomes the mere instrumentality of another—the trespasser.

Neither concept applies here. Universal makes no allegations whatsoever of duress or fraud as to visitors who mistakenly access its website. Thus, it cannot argue that YouTube intermeddled with the site. Web visitors who arrived at utube.com may have been mistaken, and YouTube may have realized that many made the same mistake; but Universal makes no allegations that site visitors were coerced or defrauded by YouTube. Universal's claim for trespass to chattel must be dismissed.

4. Nuisance

Universal alleges that YouTube operates a site that is "adjacent" to utube.com on the internet. Plaintiff asserts that YouTube's allegedly "lewd, indecent, lascivious, copyright-infringing, pornographic or obscene" videos "wrongfully interfere with or annoy plaintiff in the enjoyment of its legal rights," and that such actions constitute a nuisance.

The Restatement (Second) of Torts § 821D and other cases clearly state that nuisance involves interference with "the private use and enjoyment of land." (emphasis added).

Universal has provided virtually no legal support for its contention that a private nuisance can exist when no land is involved. Nor has Universal shown any support for the proposition that a domain name, a website, or a computer that hosts a website somehow constitutes real property. There being no such support or other basis for its nuisance claim, that claim will be dismissed.

2. Computer Misuse Law

HIQ LABS, INC. V. LINKEDIN CORP.
31 F. 4th 1180 (9th Cir. 2022)

Berzon, Circuit Judge:

We first issued an opinion in this case in September 2019, addressing the question whether LinkedIn, the professional networking website, could prevent a competitor, hiQ, from collecting and using information that LinkedIn users had shared on their public profiles, available for viewing by anyone with a web browser. hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985 (9th Cir. 2019). HiQ, a data analytics company, had obtained a preliminary injunction forbidding LinkedIn from denying hiQ access to publicly available LinkedIn member profiles. At the preliminary injunction stage, we did not resolve the companies' legal dispute definitively, nor did we address all the claims and defenses they had pleaded in the district court. Instead, we focused on whether hiQ had raised serious questions on the merits of the factual and legal issues presented to us, as well as on the other requisites for preliminary relief. We concluded that hiQ had done so, and we therefore upheld the preliminary injunction.

The Supreme Court granted LinkedIn's petition for writ of certiorari, vacated the judgment, and remanded this case for further consideration in light of Van Buren v. United States, ___ U.S. ___, 141 S. Ct. 1648, 210 L.Ed.2d 26 (2021). LinkedIn Corp. v. hiQ Labs, Inc., ___ U.S. ___, 141 S. Ct. 2752, 210 L.Ed.2d 902 (2021). We ordered supplemental briefing and held oral argument on the effect of Van Buren on this appeal. Having concluded that Van Buren reinforces our determination that hiQ has raised serious questions about whether LinkedIn may invoke the Computer Fraud and Abuse Act ("CFAA") to preempt hiQ's possibly mer-

itorious tortious interference claim, we once again affirm the preliminary injunction.

I.

Founded in 2002, LinkedIn is a professional networking website with over 500 million members. Members post resumes and job listings and build professional "connections" with other members. LinkedIn specifically disclaims ownership of the information users post to their personal profiles: according to LinkedIn's User Agreement, members own the content and information they submit or post to LinkedIn and grant LinkedIn only a non-exclusive license to "use, copy, modify, distribute, publish, and process" that information.

LinkedIn allows its members to choose among various privacy settings. Members can specify which portions of their profile are visible to the general public (that is, to both LinkedIn members and nonmembers), and which portions are visible only to direct connections, to the member's "network" (consisting of LinkedIn members within three degrees of connectivity), or to all LinkedIn members. This case deals only with profiles made visible to the general public. ...

LinkedIn has taken steps to protect the data on its website from what it perceives as misuse or misappropriation. The instructions in LinkedIn's "robots.txt" file—a text file used by website owners to communicate with search engine crawlers and other web robots—prohibit access to LinkedIn servers via automated bots, except that certain entities, like the Google search engine, have express permission from LinkedIn for bot access. LinkedIn also employs several technological systems to detect suspicious activity and restrict automated scraping. For example, LinkedIn's Quicksand system detects non-human activity indicative of scraping; its Sentinel system throttles (slows or limits) or even blocks activity from suspicious IP addresses; and its Org Block system generates a list of known "bad" IP addresses serving as large-scale scrapers. In total, LinkedIn blocks approximately 95 million automated attempts to scrape data every day, and has restricted over 11 million accounts suspected of violating its User Agreement, including through scraping.

HiQ is a data analytics company founded in 2012. Using automated bots, it scrapes information that LinkedIn users have included on public LinkedIn profiles, including name, job title, work history, and skills. It then uses that information, along with a proprietary predictive algorithm, to yield "people analytics," which it sells to business clients. ...

In recent years, LinkedIn has explored ways to capitalize on the vast amounts of data contained in LinkedIn profiles by marketing new products. In June 2017, LinkedIn's Chief Executive Officer, Jeff Weiner, appearing on CBS, explained that LinkedIn hoped to "leverage all this extraordinary data we've been able to collect by virtue of having 500 million people join the site." Weiner mentioned as possibilities providing employers with data-driven insights about what skills they will need to grow and where they can find employees with those skills. Since then, LinkedIn has announced a new product, Talent Insights, which analyzes LinkedIn data to provide companies with such data-driven information.

In May 2017, LinkedIn sent hiQ a cease-and-desist letter, asserting that hiQ was in violation of LinkedIn's User Agreement and demanding that hiQ stop accessing and copying data from LinkedIn's server. The letter stated that if hiQ accessed LinkedIn's data in the future, it would be violating state and federal law, including the CFAA, the Digital Millennium Copyright Act, California Penal Code § 502(c), and the California common law of trespass. The letter further stated that

LinkedIn had "implemented technical measures to prevent hiQ from accessing, and assisting others to access, LinkedIn's site, through systems that detect, monitor, and block scraping activity."

HiQ's response was to demand that LinkedIn recognize hiQ's right to access LinkedIn's public pages and to threaten to seek an injunction if LinkedIn refused. A week later, hiQ filed an action, seeking injunctive relief based on California law and a declaratory judgment that LinkedIn could not lawfully invoke the CFAA, the DMCA, California Penal Code § 502(c), or the common law of trespass against it. HiQ also filed a request for a temporary restraining order, which the parties subsequently agreed to convert into a motion for a preliminary injunction.

The district court granted hiQ's motion. It ordered LinkedIn to withdraw its cease-and-desist letter, to remove any existing technical barriers to hiQ's access to public profiles, and to refrain from putting in place any legal or technical measures with the effect of blocking hiQ's access to public profiles. LinkedIn timely appealed.

II.

"A plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest." *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 20, (2008). All four elements must be satisfied.

A. Irreparable Harm

[The court held that HiQ had established that it was likely to suffer irreparable harm due to its inability to serve its existing clients.]

B. Balance of the Equities ...

On one side of the scale is the harm to hiQ just discussed: the likelihood that, without an injunction, it will go out of business. On the other side, LinkedIn asserts that the injunction threatens its members' privacy and therefore puts at risk the goodwill LinkedIn has developed with its members. As the district court observed, "the fact that a user has set his profile to public does not imply that he wants any third parties to collect and use that data for all purposes." LinkedIn points in particular to the more than 50 million members who have used the "Do Not Broadcast" feature to ensure that other users are not notified when the member makes a profile change. According to LinkedIn, the popularity of the "Do Not Broadcast" feature indicates that many members—including members who choose to share their information publicly—do not want their employers to know they may be searching for a new job. An employer who learns that an employee may be planning to leave will not necessarily reward that employee with a retention bonus. Instead, the employer could decide to limit the employee's access to sensitive information or even to terminate the employee.

There is support in the record for the district court's connected conclusions that (1) LinkedIn's assertions have some merit; and (2) there are reasons to discount them to some extent. First, there is little evidence that LinkedIn users who choose to make their profiles public actually maintain an expectation of privacy with respect to the information that they post publicly, and it is doubtful that they do. LinkedIn's privacy policy clearly states that "any information you put on your profile and any content you post on LinkedIn may be seen by others" and instructs users not to "post or add personal data to your profile that you would not want to be public."

Second, there is no evidence in the record to suggest that most people who select the "Do Not Broadcast" option do so to prevent their employers from being alerted to profile changes made in anticipation of a job search. As the district court stated, there are other reasons why users may choose that option—most notably, many users may simply wish to avoid sending their connections annoying notifications each time there is a profile change. In any event, employers can always directly consult the profiles of users who chose to make their profiles public to see if any recent changes have been made. Employees intent on keeping such information from their employers can do so by rejecting public exposure of their profiles and eliminating their employers as contacts.

Finally, LinkedIn's own actions undercut its argument that users have an expectation of privacy in public profiles. LinkedIn's "Recruiter" product enables recruiters to "follow" prospects, get "alerted when prospects make changes to their profiles," and "use those alerts as signals to reach out at just the right moment," without the prospect's knowledge. And subscribers to LinkedIn's "talent recruiting, marketing and sales solutions" can export data from members' public profiles, such as "name, headline, current company, current title, and location."

In short, even if some users retain some privacy interests in their information notwithstanding their decision to make their profiles public, we cannot, on the record before us, conclude that those interests— or more specifically, LinkedIn's interest in preventing hiQ from scraping those profiles—are significant enough to outweigh hiQ's interest in continuing its business, which depends on accessing, analyzing, and communicating information derived from public LinkedIn profiles.

Nor do the other harms asserted by LinkedIn tip the balance of harms with regard to preliminary relief. LinkedIn invokes an interest in preventing "free riders" from using profiles posted on its platform. But LinkedIn has no protected property interest in the data contributed by its users, as the users retain ownership over their profiles. And as to the publicly available profiles, the users quite evidently intend them to be accessed by others, including for commercial purposes—for example, by employers seeking to hire individuals with certain credentials. Of course, LinkedIn could satisfy its "free rider" concern by eliminating the public access option, albeit at a cost to the preferences of many users and, possibly, to its own bottom line. ...

C. Likelihood of Success

Because hiQ has established that the balance of hardships tips decidedly in its favor, the likelihood-of-success prong of the preliminary injunction inquiry focuses on whether hiQ has raised serious questions going to the merits. It has. ...

1. Tortious Interference with Contract

HiQ alleges that LinkedIn intentionally interfered with hiQ's contracts with third parties. "The elements which a plaintiff must plead to state the cause of action for intentional interference with contractual relations are (1) a valid contract between plaintiff and a third party; (2) defendant's knowledge of this contract; (3) defendant's intentional acts designed to induce a breach or disruption of the contractual relationship; (4) actual breach or disruption of the contractual relationship; and (5) resulting damage." *Pac. Gas & Elec. Co. v. Bear Stearns & Co.*, 50 Cal. 3d 1118, 1126 (1990).

HiQ has shown a sufficient likelihood of establishing each of these elements. First, LinkedIn does not contest hiQ's evidence that contracts exist between hiQ and some customers, including eBay, Capital One, and GoDaddy.

Second, hiQ will likely be able to establish that LinkedIn knew of hiQ's scraping activity and products for some time. LinkedIn began sending representatives to hiQ's Elevate conferences in October 2015. ...

Third, LinkedIn's threats to invoke the CFAA and implementation of technical measures selectively to ban hiQ bots could well constitute "intentional acts designed to induce a breach or disruption" of hiQ's contractual relationships with third parties. Pac. Gas & Elec. Co., 50 Cal. 3d at 1126.

Fourth, the contractual relationships between hiQ and third parties have been disrupted and now hang in the balance. Without access to LinkedIn data, hiQ will likely be unable to deliver its services to its existing customers as promised.

Last, hiQ is harmed by the disruption to its existing contracts and interference with its pending contracts. Without the revenue from sale of its products, hiQ will likely go out of business.

LinkedIn does not specifically challenge hiQ's ability to make out any of these elements of a tortious interference claim. Instead, LinkedIn maintains that it has a "legitimate business purpose" defense to any such claim. *Cf. Quelimane Co. v. Stewart Title Guar. Co.*, 19 Cal. 4th 26, 57 (1998). That contention is an affirmative justification defense for which LinkedIn bears the burden of proof. ...

California courts apply a balancing test to determine whether the interests advanced by interference with contract outweigh the societal interest in contractual stability:

> Whether an intentional interference by a third party is justifiable depends upon a balancing of the importance, social and private, of the objective advanced by the interference against the importance of the interest interfered with, considering all circumstances including the nature of the actor's conduct and the relationship between the parties.

Herron v. State Farm Mut. Ins. Co., 56 Cal. 2d 202, 206 (1961). ...

Balancing the interest in contractual stability and the specific interests interfered with against the interests advanced by the interference, we agree with the district court that hiQ has at least raised a serious question on the merits of LinkedIn's affirmative justification defense. First, hiQ has a strong commercial interest in fulfilling its contractual obligations to large clients like eBay and Capital One. Those companies benefit from hiQ's ability to access, aggregate, and analyze data from LinkedIn profiles.

Second, LinkedIn's means of interference is likely not a "recognized trade practice" as California courts have understood that term. "Recognized trade practices" include such activities as "advertising," "price-cutting," and "hiring the employees of another for use in the hirer's business," *Buxbom*, 23 Cal. 2d at 546-47, 145 P.2d 305—all practices which may indirectly interfere with a competitor's contracts but do not fundamentally undermine a competitor's basic business model. LinkedIn's proactive technical measures to selectively block hiQ's access to the data on its site are not similar to trade practices previously recognized as acceptable justifications for contract interference.

Further, LinkedIn's conduct may well not be within the realm of fair competition. HiQ has raised serious questions about whether LinkedIn's actions to ban hiQ's bots were taken in furtherance of LinkedIn's own plans to introduce a competing professional data analytics tool. There is evidence from which it can be inferred that LinkedIn knew about hiQ and its reliance on external data for several years before the present controversy. Its decision to send a cease-and-desist letter occurred within a month of the announcement by LinkedIn's CEO that LinkedIn

planned to leverage the data on its platform to create a new product for employers with some similarities to hiQ's Skill Mapper product. If companies like LinkedIn, whose servers hold vast amounts of public data, are permitted selectively to ban only potential competitors from accessing and using that otherwise public data, the result—complete exclusion of the original innovator in aggregating and analyzing the public information—may well be considered unfair competition under California law.

Finally, LinkedIn's asserted private business interests—"protecting its members' data and the investment made in developing its platform" and "enforcing its User Agreements' prohibitions on automated scraping"—are relatively weak. LinkedIn has only a non-exclusive license to the data shared on its platform, not an ownership interest. Its core business model—providing a platform to share professional information—does not require prohibiting hiQ's use of that information, as evidenced by the fact that hiQ used LinkedIn data for some time before LinkedIn sent its cease-and-desist letter. As to its members' interests in their data, for the reasons already explained, we agree with the district court that members' privacy expectations regarding information they have shared in their public profiles are "uncertain at best." Further, there is evidence that LinkedIn has itself developed a data analytics tool similar to HiQ's products, undermining LinkedIn's claim that it has its members' privacy interests in mind. Finally, LinkedIn has not explained how it can enforce its user agreement against hiQ now that its user status has been terminated.

For all these reasons, LinkedIn may well not be able to demonstrate a "legitimate business purpose" that could justify the intentional inducement of a contract breach, at least on the record now before us. ...

2. Computer Fraud and Abuse Act (CFAA) ...

LinkedIn argues that even if hiQ can show a likelihood of success on any of its state law causes of action, all those causes of action are preempted by the CFAA, 18 U.S.C. § 1030, which LinkedIn asserts that hiQ violated.

The CFAA states that "whoever ... intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... information from any protected computer ... shall be punished" by fine or imprisonment. 18 U.S.C. § 1030(a)(2)(C). The term "protected computer" refers to any computer "used in or affecting interstate or foreign commerce or communication," 18 U.S.C. § 1030(e)(2)(B)—effectively any computer connected to the Internet, see *United States v. Nosal* (*Nosal II)*, 844 F.3d 1024, 1050 (9th Cir. 2016)—including servers, computers that manage network resources and provide data to other computers. LinkedIn's computer servers store the data members share on LinkedIn's platform and provide that data to users who request to visit its website. Thus, to scrape LinkedIn data, hiQ must access LinkedIn servers, which are protected computers.

The pivotal CFAA question here is whether once hiQ received LinkedIn's cease-and-desist letter, any further scraping and use of LinkedIn's data was "without authorization" within the meaning of the CFAA and thus a violation of the statute. If so, LinkedIn maintains, hiQ could have no legal right of access to LinkedIn's data and so could not succeed on any of its state law claims, including the tortious interference with contract claim we have held otherwise sufficient for preliminary injunction purposes.

We have held in another context that the phrase "'without authorization' is a non-technical term that, given its plain and ordinary meaning, means accessing a protected computer without permission." *Nosal II,* 844 F.3d at 1028. *Nosal II* in-

volved an employee accessing without permission an employer's private computer for which access permissions in the form of user accounts were required. *Nosal II* did not address whether access can be "without authorization" under the CFAA where, as here, prior authorization is not generally required, but a particular person—or bot—is refused access. HiQ's position is that *Nosal II* is consistent with the conclusion that where access is open to the general public, the CFAA "without authorization" concept is inapplicable. At the very least, we conclude, hiQ has raised a serious question as to this issue.

First, the wording of the statute, forbidding "access ... without authorization," 18 U.S.C. § 1030(a)(2), suggests a baseline in which access is not generally available and so permission is ordinarily required. "Authorization" is an affirmative notion, indicating that access is restricted to those specially recognized or admitted. Where the default is free access without authorization, in ordinary parlance one would characterize selective denial of access as a ban, not as a lack of "authorization."

Second, even if this interpretation is debatable, the legislative history of the statute confirms our understanding.

The CFAA was enacted to prevent intentional intrusion onto someone else's computer—specifically, computer hacking. See *United States v. Nosal* (*Nosal I*), 676 F.3d 854, 858 (9th Cir. 2012).

The 1984 House Report on the CFAA explicitly analogized the conduct prohibited by section 1030 to forced entry: "It is noteworthy that section 1030 deals with an 'unauthorized access' concept of computer fraud rather than the mere use of a computer. Thus, the conduct prohibited is analogous to that of 'breaking and entering.'" H.R. Rep. No. 98-894, at 20 (1984); *see also id.* at 10 (describing the problem of "'hackers' who have been able to access (trespass into) both private and public computer systems"). Senator Jeremiah Denton similarly characterized the CFAA as a statute designed to prevent unlawful intrusion into otherwise inaccessible computers, observing that "[t]he bill makes it clear that unauthorized access to a Government computer is a trespass offense, as surely as if the offender had entered a restricted Government compound without proper authorization." 132 Cong. Rec. 27639 (1986). And when considering amendments to the CFAA two years later, the House again linked computer intrusion to breaking and entering. See H.R. Rep. No. 99-612, at 5-6 (1986) (describing ""he expanding group of electronic trespassers," who trespass "just as much as if they broke a window and crawled into a home while the occupants were away").

In recognizing that the CFAA is best understood as an anti-intrusion statute and not as a "misappropriation statute," *Nosal I*, 676 F.3d at 857-58, we rejected the contract-based interpretation of the CFAA's "without authorization" provision adopted by some of our sister circuits. *Compare Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067 (9th Cir. 2016) ("A violation of the terms of use of a website—without more—cannot establish liability under the CFAA."); *Nosal I*, 676 F.3d at 862 ("We remain unpersuaded by the decisions of our sister circuits that interpret the CFAA broadly to cover violations of corporate computer use restrictions or violations of a duty of loyalty."), with *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 583-84 (1st Cir. 2001) (holding that violations of a confidentiality agreement or other contractual restraints could give rise to a claim for unauthorized access under the CFAA); *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010) (holding that a defendant "exceeds authorized access" when violating policies governing authorized use of databases). *Van Buren*, interpreting the

CFAA's "exceeds authorized access" clause, approved of *Nosal I* and abrogated *EF Cultural Travel* and *Rodriguez*. 141 S. Ct. at 1653-54 & n.2.

We therefore look to whether the conduct at issue is analogous to breaking and entering. Significantly, the version of the CFAA initially enacted in 1984 was limited to a narrow range of computers—namely, those containing national security information or financial data and those operated by or on behalf of the government. None of the computers to which the CFAA initially applied were accessible to the general public; affirmative authorization of some kind was presumptively required.

When section 1030(a)(2)(C) was added in 1996 to extend the prohibition on unauthorized access to any "protected computer," the Senate Judiciary Committee explained that the amendment was designed "to increase protection for the privacy and confidentiality of computer information." S. Rep. No. 104-357, at 7. The legislative history of section 1030 thus makes clear that the prohibition on unauthorized access is properly understood to apply only to private information—information delineated as private through use of a permission requirement of some sort. As one prominent commentator has put it, "an authentication requirement, such as a password gate, is needed to create the necessary barrier that divides open spaces from closed spaces on the Web." Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1161 (2016). Moreover, elsewhere in the statute, password fraud is cited as a means by which a computer may be accessed without authorization, see 18 U.S.C. § 1030(a)(6), bolstering the idea that authorization is only required for password-protected sites or sites that otherwise prevent the general public from viewing the information.

We therefore conclude that hiQ has raised a serious question as to whether the reference to access "without authorization" limits the scope of the statutory coverage to computers for which authorization or access permission, such as password authentication, is generally required. Put differently, the CFAA contemplates the existence of three kinds of computer systems: (1) computers for which access is open to the general public and permission is not required, (2) computers for which authorization is required and has been given, and (3) computers for which authorization is required but has not been given (or, in the case of the prohibition on exceeding authorized access, has not been given for the part of the system accessed). Public LinkedIn profiles, available to anyone with an Internet connection, fall into the first category. With regard to websites made freely accessible on the Internet, the "breaking and entering" analogue invoked so frequently during congressional consideration has no application, and the concept of "without authorization" is inapt.

The reasoning of *Van Buren* reinforces our interpretation of the CFAA, although it did not directly address the statute's "without authorization" clause. Van Buren held that a police sergeant did not violate the CFAA when he "ran a license-plate search in a law enforcement computer database in exchange for money." 141 S. Ct. at 1652. Interpreting the "exceeds authorized access" clause of section 1030(a)(2), the Court held that the CFAA "covers those who obtain information from particular areas in the computer—such as files, folders, or databases—to which their computer access does not extend. It does not cover those who, like Van Buren, have improper motives for obtaining information that is otherwise available to them." *Id.*

Van Buren found the "interplay between the 'without authorization' and 'exceeds authorized access' clauses of subsection (a)(2) ... particularly probative." *Id.*

at 1658. "The without authorization' clause ... protects computers themselves by targeting so-called outside hackers—those who access a computer without any permission at all." *Id.* The "'exceeds authorized access' clause ... provides complementary protection for certain information within computers ... by targeting so-called inside hackers—those who access a computer with permission, but then "'exceed" the parameters of authorized access by entering an area of the computer to which [that] authorization does not extend.'" *Id.* "Liability under both clauses stems from a gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system." *Id.* at 1658-59.

Van Buren's "gates-up-or-down inquiry" is consistent with our interpretation of the CFAA as contemplating three categories of computer systems. Discussing the "without authorization" clause, *Van Buren* explained that a computer user who has "authorization" is one who "can ... access a computer system," 141 S. Ct. at 1658, where "access" means "the act of entering a computer 'system itself,'" *id.* at 1657. In other words, a user with "authorization" is not subject to "limitations on access," whether those limitations are "code-based" or "contained in contracts or policies." *Id.* at 1659 n.8. ...

Van Buren's distinction between computer users who "can or cannot access a computer system," *id.* at 1658, suggests a baseline in which there are "limitations on access" that prevent some users from accessing the system (i.e., a "gate" exists, and can be either up or down). The Court's "gates-up-or-down inquiry" thus applies to the latter two categories of computers we have identified: if authorization is required and has been given, the gates are up; if authorization is required and has not been given, the gates are down. As we have noted, however, a defining feature of public websites is that their publicly available sections lack limitations on access; instead, those sections are open to anyone with a web browser. In other words, applying the "gates" analogy to a computer hosting publicly available webpages, that computer has erected no gates to lift or lower in the first place. *Van Buren* therefore reinforces our conclusion that the concept of "without authorization" does not apply to public websites.

Additionally, neither of the cases LinkedIn principally relies upon casts doubt on our interpretation of the statute. LinkedIn first cites *Nosal II.* As we have already stated, *Nosal II* held that a former employee who used current employees' login credentials to access company computers and collect confidential information had acted "'without authorization' in violation of the CFAA." 844 F.3d at 1038. The computer information the defendant accessed in *Nosal II* was thus plainly one which no one could access without authorization.

So too with regard to the system at issue in *Power Ventures*, 844 F.3d 1058, the other precedent upon which LinkedIn relies. In that case, Facebook sued Power Ventures, a social networking website that aggregated social networking information from multiple platforms, for accessing Facebook users' data and using that data to send mass messages as part of a promotional campaign. After Facebook sent a cease-and-desist letter, Power Ventures continued to circumvent IP barriers and gain access to password-protected Facebook member profiles. We held that after receiving an individualized cease-and-desist letter, Power Ventures had accessed Facebook computers "without authorization" and was therefore liable under the CFAA. But we specifically recognized that "Facebook has tried to limit and control access to its website" as to the purposes for which Power Ventures sought to use it. *Id.* at 1063. Indeed, Facebook requires its users to register with a unique

username and password, and Power Ventures required that Facebook users provide their Facebook username and password to access their Facebook data on Power Ventures' platform. While Power Ventures was gathering user data that was protected by Facebook's username and password authentication system, the data hiQ was scraping was available to anyone with a web browser.

In sum, *Nosal II* and *Power Ventures* control situations in which authorization generally is required and has either never been given or has been revoked. As *Power Ventures* indicated, the two cases do not control the situation present here, in which information is presumptively open to all comers. As to the computers at issue in those cases, the authorization gate was "down." ...

For all these reasons, it appears that the CFAA's prohibition on accessing a computer "without authorization" is violated when a person circumvents a computer's generally applicable rules regarding access permissions, such as username and password requirements, to gain access to a computer. It is likely that when a computer network generally permits public access to its data, a user's accessing that publicly available data will not constitute access without authorization under the CFAA. The data hiQ seeks to access is not owned by LinkedIn and has not been demarcated by LinkedIn as private using such an authorization system. HiQ has therefore raised serious questions about whether LinkedIn may invoke the CFAA to preempt hiQ's possibly meritorious tortious interference claim.

Entities that view themselves as victims of data scraping are not without resort, even if the CFAA does not apply: state law trespass to chattels claims may still be available. And other causes of action, such as copyright infringement, misappropriation, unjust enrichment, conversion, breach of contract, or breach of privacy, may also lie. *See, e.g.*, *Associated Press v. Meltwater U.S. Holdings, Inc.*, 931 F. Supp. 2d 537, 561 (S.D.N.Y. 2013) (holding that a software company's conduct in scraping and aggregating copyrighted news articles was not protected by fair use).

D. Public Interest

Finally, we must consider the public interest in granting or denying the preliminary injunction. ...

As the district court observed, each side asserts that its own position would benefit the public interest by maximizing the free flow of information on the Internet. HiQ points out that data scraping is a common method of gathering information, used by search engines, academic researchers, and many others. According to hiQ, letting established entities that already have accumulated large user data sets decide who can scrape that data from otherwise public websites gives those entities outsized control over how such data may be put to use.

For its part, LinkedIn argues that the preliminary injunction is against the public interest because it will invite malicious actors to access LinkedIn's computers and attack its servers. As a result, the argument goes, LinkedIn and other companies with public websites will be forced to choose between leaving their servers open to such attacks or protecting their websites with passwords, thereby cutting them off from public view.

Although there are significant public interests on both sides, the district court properly determined that, on balance, the public interest favors hiQ's position. We agree with the district court that giving companies like LinkedIn free rein to decide, on any basis, who can collect and use data—data that the companies do not own, that they otherwise make publicly available to viewers, and that the companies themselves collect and use—risks the possible creation of information monopolies that would disserve the public interest.

Internet companies and the public do have a substantial interest in thwarting denial-of-service attacks and blocking abusive users, identity thieves, and other ill-intentioned actors. But we do not view the district court's injunction as opening the door to such malicious activity. The district court made clear that the injunction does not preclude LinkedIn from continuing to engage in "technological self-help" against bad actors—for example, by employing "anti-bot measures to prevent, e.g., harmful intrusions or attacks on its server." Although an injunction preventing a company from securing even the public parts of its website from malicious actors would raise serious concerns, such concerns are not present here.

The district court's conclusion that the public interest favors granting the preliminary injunction was appropriate.

3. Contract Law

HIQ LABS, INC. V. LINKEDIN CORP.
639 F. Supp. 3d 944 (N.D. Cal. 2022)

[On remand, the district court considered various issues, including LinkedIn's breach of contract claim.]

Chen, District Judge: ...

A. Breach Of Contract

LinkedIn moves for partial summary judgment on its breach of contract claim for (1) hiQ's scraping of LinkedIn's site and using the collected data to sell its Keeper and Skill Mapper products, and (2) hiQ's use and for directing "turkers" to make fake accounts and to copy url data as part of hiQ's scraping operation. hiQ only contests the breach and damages elements. Specifically, as to the first accused conduct, hiQ argues that questions of fact remain as to whether the User Agreement is ambiguous and consequently whether hiQ breached that Agreement. For the turkers' actions, hiQ argues that they did not constitute a breach that resulted in damages and that it was not responsible for them. hiQ also argues that its affirmative defenses bar the breach claim.

1. Liability

a. Scraping and Using Collected Data

LinkedIn's User Agreement expressly prohibits scraping of its site. Section 8 of the User Agreement ("LinkedIn 'DOs' and 'DON'Ts'") states:

> 8.2 Don'ts. You agree that you will not: ...
>
> - Scrape or copy profiles and information of others through any means (including crawlers, browser plugins and add-ons, and any other technology or manual work); ...
> - Use manual or automated software, devices, scripts, robots, other means or processes to access, "scrape," "crawl" or "spider" the Services or any related data or information;
> - Use bots or other automated methods to access the Services, add or download contracts, send or redirect messages; ...

As relevant to hiQ's argument, the User Agreement also delineates members' rights and obligations as follows:

> 2. Obligations ...

> When you share information, others can see, copy and use that information. ...
>
> 3.1 Your License to LinkedIn ...
>
> c. We will get your consent if we want to give others the right to publish your posts beyond the Service. However, other Members and/or Visitors may access and share your content and information, consistent with your settings and degree of connection with them. ...

Despite the clear language cited above, hiQ argues that LinkedIn's User Agreement was nonetheless ambiguous because of (1) inconsistent provisions within the Agreement, and (2) extrinsic evidence, including LinkedIn's conduct which suggested that scraping was not categorically barred. ...

User Agreement Provisions. Contrary to hiQ's characterization, the User Agreement's provisions do not conflict with each other. According to hiQ, the User Agreement's statements that "Visitors may access and share your content and information consistent with your settings" and that "when you share information, others can see, copy and use that information" are inconsistent with the prohibition of scraping data—a means to access and copy LinkedIn members' information. Thus, hiQ argues that the inconsistency creates a question of fact as to whether its conduct constitutes a breach of the User Agreement.

The Court disagrees. Informing members that their data may be "see[n], cop[ied], and use[d]" does not contradict the prohibition against "scrap[ing], crawl[ing], or spider[ing] the Server." The two concepts are not mutually exclusive—a warning to members that a third party may collect their public-facing data is not a blessing for third parties to do so through expressly prohibited means. Thus, the contract's language itself does not create ambiguity within the User Agreement.

Extrinsic Evidence. hiQ's extrinsic evidence includes an internal email between LinkedIn employees stating that LinkedIn "generally do[es]n't pursue cases of public scraping," the fact that LinkedIn scraped its competitor's websites, and the fact that LinkedIn's parent company scraped LinkedIn. Also, hiQ argues that LinkedIn's non-enforcement implied that the agreement does not bar scraping.

However, parol evidence is admissible only to prove a meaning to which the language is reasonably susceptible, not to flatly contradict the express terms of the agreement. hiQ seeks to introduce parol evidence to prove that it may "[u]se manual or automated software, devices, scripts[,] robots ... to access, 'scrape,' 'crawl' or 'spider' the [LinkedIn] Services" even though the User Agreement says hiQ "agree[d] that [it] will not" do so. (User Agreement § 8.2.) That extrinsic evidence does not negate or diminish the express terms of the User Agreement. Furthermore, LinkedIn's failure to abide by or enforce the Agreement, which perhaps gives rise to an affirmative defense, does not contradict or render ambiguous the unambiguous terms of the Agreement.

In sum, the relevant language of the User Agreement unambiguously prohibits hiQ's scraping and unauthorized use of the scraped data.

b. Turkers

hiQ argues against liability for the turkers' conduct because (1) no evidence shows that the turkers ever scraped any profile information, (2) it is not responsible for its independent contractors' acts, and (3) no evidence shows actual harm.

Undisputed evidence shows that hiQ's turkers registered false LinkedIn identities under its instructions in breach of the User Agreement. Section 8 of the User Agreement ("LinkedIn 'DOs' and 'DON'Ts'") states:

> 8.2 Don'ts. You agree that you will not: ...
>
> - Create a false identity on LinkedIn; ...

hiQ's turker training document for the Keeper product explicitly instructed, "It is a good idea to make a fake account with a fake email, to deal with the possibility of being banned on LinkedIn." Undisputed evidence suggests that turkers followed this instruction. Regardless of whether the turkers scraped LinkedIn's site, they breached the User Agreement's prohibition on creating false identities.

Although turkers were hiQ's independent contractors, hiQ cannot escape liability because they also acted as its agent regarding the log-in process to LinkedIn.

Here, undisputed evidence shows that hiQ retained a high degree of control over turkers' log-in process. Its training documents provided suggestions on how to log into LinkedIn's accounts. *See, e.g.,* LCE 0151 ("It is a good idea to make a fake account with a fake email, to deal with the possibility of being banned on LinkedIn."); HCE Ex. 102 ("Log into linkedin.com, you may want to create new accounts for turking to avoid having your account harassed. It is important that you are browsing anonymously."). When LinkedIn "cracked down on usage in a way that [wa]s making problems for turking," hiQ "instruct[ed] turkers on how to proceed." (LCE 1048 (hiQ email).) hiQ itself considered the turkers their agents. (LCE 0328 (hiQ internal email stating, "by turking *we* may be violating some of [LinkedIn's] terms of use, such as the requirement that users of LinkedIn don't create false identities and will use their real names on their profiles") (emphasis added).) hiQ has not pointed to contrary evidence regarding its control over the turkers' logging in process. There is no dispute then that turkers thus acted as hiQ's agents and their liabilities accrue to it. *See* Cal. Civ. Code § 2330 ("An agent represents his principal for all purposes within the scope of his actual or ostensible authority, and all the rights and liabilities which would accrue to the agent from transactions within such limit, if they had been entered into on his own account, accrue to the principal.").

Finally, although hiQ contends LinkedIn suffered no damages from turkers' actions, nominal damages are available for breach of contract and can support entry of judgment in favor of a plaintiff who suffered no appreciable harm. hiQ has therefore breached LinkedIn's User Agreement through the turkers' conduct.

c. Summary

In sum, hiQ breached LinkedIn's User Agreement both through its own scraping of LinkedIn's site and using scraped data, and through turkers' creation of false identities on LinkedIn's platform.

CVENT, INC. V. EVENTBRITE, INC.

739 F.Supp.2d 927 (E.D. Va. 2010)

Brinkema, District Judge: ...

Before the Court is defendant Eventbrite's motion to dismiss several of the counts in the plaintiff's first amended complaint for failure to state a claim. For the reasons stated in open court and in this opinion, the defendant's motion will be granted in part and denied in part.

I. BACKGROUND ...

Cvent is the owner and operator of a website at www.cvent.com, which, among other things, assists customers in locating venues for and organizing large-scale events. As part of that business; Cvent has created a web-based database of meeting venues around the world, called the Cvent Supplier Network, which includes detailed information about each venue, such as the availability and capacity of meeting rooms and venue amenities and services. ...

Defendant Eventbrite, Inc. is a Delaware corporation with its principal place of business in San Francisco, California, which maintains an online event planning, sales, and registration service hosted on its website, www.eventbrite.com. Cvent alleges that in September and October 2008, Eventbrite set out to create a set of pages on its website containing a collection of publicly available information about hotels, restaurants, bars, and meeting venues in various cities. Most of the information in Eventbrite's Venue Directory is publicly available from the website of each hotel and restaurant. Cvent alleges that rather than aggregating that information itself, Eventbrite hired Stephan Foley, a computer engineer, to "scrape" the information directly from Cvent's website. Cvent further alleges that Eventbrite then reformatted the material into its own layouts and made it available on the Eventbrite website. ...

III. DISCUSSION ...

The gravamen of Cvent's complaint is, at its core, a claim for intellectual property theft and copyright infringement. Accordingly, Eventbrite does not move to dismiss plaintiff's Copyright Act claim, nor could it plausibly do so under Fed. R. Civ. P. 12(b)(6). However, plaintiff has also raised seven other claims premised upon state and federal law, both statutory and common law, all of which Eventbrite moves to dismiss. ...

A. Claim Two: Computer Fraud and Abuse Act, 18 U.S.C. § 1030

Eventbrite moves to dismiss the Computer Fraud and Abuse Act (CFAA) claim on the ground that the CFAA only prohibits hacking or other unauthorized access to files, while the material that Eventbrite is alleged to have scraped from Cvent's website is publicly available, and Eventbrite was thus authorized to access it. ...

Eventbrite moves to dismiss this count on the ground that although Cvent may have pled facts giving rise to a plausible inference that defendants made an unauthorized use of the material on the Cvent website, the complaint does not allege sufficient facts to support a claim that defendants obtained unauthorized *access* to that information. Rather, the data which Eventbrite is alleged to have stripped from Cvent's website is publicly available on the Internet, without requiring any login, password, or other individualized grant of access. By definition, therefore, Eventbrite argues it could not have "exceeded" its authority to access that data.

Cvent's only argument in support of its CFAA claim rests upon the Terms of Use on its website, which state in part that "No competitors or future competitors are permitted access to our site or information, and any such access by third parties is unauthorized...." Notwithstanding that language, Cvent's website in fact takes no affirmative steps to screen competitors from accessing its information. Cvent's CSN venue location database is not password-protected, nor are users of the website required to manifest assent to the Terms of Use, such as by clicking "I agree" before gaining access to the database. Rather, anyone, including competitors in the field of event planning, may access and search event's venue information at will.

Indeed, the Terms of Use for event's website are not displayed on the website in any way in which a reasonable user could be expected to notice them. Based upon screenshots of the website provided to the Court by defense counsel, and to which plaintiff's counsel did not object, the Terms of Use do not themselves appear in the body of the first page of the Cvent website. The link that accesses the Terms is buried at the bottom of the first page, in extremely fine print, and users must affirmatively scroll down to the bottom of the page to even see the link. Specifically, when users scroll down to the bottom of Cvent's homepage, they are confronted with a black band with twenty-eight different links separated into four columns and grouped under four headings: "Event Planning," "Online Surveys," "Site Selection," and "Company Info." Under the "Company Info" heading, the rightmost heading on the page, the "Terms of Use" link appears two lines down in small white font, sandwiched between "Privacy Policy" and "Contact Us," Moreover, even when users click on "Terms of Use," they are directed to a secondary page entitled "Terms of Use for Cvent Products," which itself has three separate links to three different Terms of Use: "Supplier Network Terms of Use," "Event Management Terms of Use," and "Web Survey Terms of Use." Website users can access the various Terms of Use documents only by clicking on the appropriate links, thereby opening the documents on a new page. The documents themselves are each several pages long.

Cvent's website, including its CSN database, is therefore not protected in any meaningful fashion by its Terms of Use or otherwise. Eventbrite thus properly cites to *State Analysis, Inc. v. American Financial Services, Assoc.*, 621 F. Supp.2d 309 (E.D. Va. 2009) (Brinkema, J.), in which this Court rejected a CFAA claim against a defendant who, like Eventbrite, was accused of using material to which it had lawful access in ways that violated the agreement governing that access. In *State Analysis,* the plaintiff sued two defendants: the first was alleged to have accessed the plaintiff's website using usernames and passwords that did not belong to it and to which it had never been given lawful access, while the second was alleged to have misused the passwords with which it had been entrusted. This Court allowed the CFAA claim to proceed against the first defendant, but granted the second defendant's motion to dismiss, explicitly-holding that while use of an unauthorized password to access password-protected content may constitute a CFAA violation, a mere allegation that a defendant "used the information [which it had been given lawful authority to access] in an inappropriate way" did not state a claim for relief. *Id.* at 317.

The overwhelming weight of authority supports this view of the CFAA.Meanwhile, the cases cited by Cvent in its opposition to Eventbrite's motion to dismiss nearly all present factual situations that are distinguishable from the facts in the instant case. For example, *America Online v. LCGM, Inc.*, 46 F. Supp.2 d 444 (E.D. Va. 1998), the only case cited by plaintiff from this district, upheld a CFAA claim for electronic datastripping. However, the defendants in that case were alleged to have obtained AOL e-mail accounts in order to use extractor software programs to harvest the e-mail addresses of AOL members and then send bulk spam solicitations to them. *Id.* at 448. Not only was such conduct in violation of AOL's Terms of Use, but the defendants were plainly never given authorized access to the confidential e-mail addresses of other users. The *AOL* case thus stands in contradistinction to this case, where the entire world was given unimpeded access to Cvent's website, its CSN venue database, and its "Destination Guide." For those reasons, Eventbrite's motion to dismiss plaintiff's CFAA claim will be granted. ...

D. Claim Five: Breach of Contract

Eventbrite next moves to dismiss plaintiff's breach of contract claim for failure to state a plausible entitlement to relief. Eventbrite sets forth three arguments in support of that motion: (1) any contract claim against Eventbrite is preempted by federal copyright law; (2) Eventbrite is not a party to any contract; and (3) no contract exists.

The first two arguments are unavailing. A breach of contract claim premised upon the Terms of Use on Cvent's website is qualitatively different from a claim for copyright infringement under the Copyright Act and therefore is not preempted. Moreover, as explained below with respect to plaintiff's conspiracy claims, Cvent has explicitly pled that defendant Foley was an agent of defendant Eventbrite, which hired Foley as an independent contractor to perform the alleged "website scraping" conduct at issue here. Thus, to the extent that any contract exists, Foley's assent to that contract would bind Eventbrite, the principal.

However, Cvent's breach of contract claim fails to state an entitlement to legal relief because Cvent has not alleged sufficient facts to support a plausible allegation that a contract existed between Cvent and Eventbrite. Plaintiff's complaint fails to allege any written or oral contract between the parties. Instead, Cvent relies exclusively on its "Terms of Use," which are displayed on secondary pages of its website and can be accessed only through one of several dozen small links at the bottom of the first page. As noted above in this Court's analysis with respect to plaintiff's Computer Fraud and Abuse Act claim, on pages 8-9 of this Memorandum Opinion, the "Terms of Use" link only appears on Cvent's website via a link buried at the bottom of the first page. Moreover, users of event's website are not required to click on that link, nor are they required to read or assent to the Terms of Use in order to use the website or access any of its content. This case is therefore not a "clickwrap" case, but rather falls into a category of alleged contracts that many courts have termed "browsewrap agreements."

Neither party in this case has cited case law from either the Fourth Circuit or this Court explicitly addressing the validity of this type of browsewrap contract. Most courts which have considered the issue, however, have held that in order to state a plausible claim for relief based upon a browsewrap agreement, the website user must have had actual or constructive knowledge of the site's terms and conditions, and have manifested assent to them. In this case, plaintiff has not pled sufficient facts to plausibly establish that defendants Eventbrite and Foley were on actual or constructive notice of the terms and conditions posted on Cvent's website. ...

REGISTER. COM, INC. V. VERIO, INC.
356 F. 3d 393 (2d Cir. 2004)

Leval, Circuit Judge: ...

BACKGROUND

This plaintiff Register is one of over fifty companies serving as registrars for the issuance of domain names on the world wide web. As a registrar, Register issues domain names to persons and entities preparing to establish web sites on the Internet. Web sites are identified and accessed by reference to their domain names.

[Register's contract with the Internet Corporation for Assigned Names and Numbers (ICANN), which administers the domain-name system, obligated Register to "provide for free public access" to "WHOIS" data, consisting of registrants' "name, postal address, telephone number, and electronic mail address." Register

did so through what in modern terms would be called a service or API known as "port 43."]

An entity making a WHOIS query through Register's Internet site or port 43 would receive a reply furnishing the requested WHOIS information, captioned by a legend devised by Register, which stated,

> By submitting a WHOIS query, you agree that you will use this data only for lawful purposes and that under no circumstances will you use this data to ... support the transmission of mass unsolicited, commercial advertising or solicitation via email. ...

The defendant Verio, against whom the preliminary injunction was issued, is engaged in the business of selling a variety of web site design, development and operation services. In the sale of such services, Verio competes with Register's web site development business. To facilitate its pursuit of customers, Verio undertook to obtain daily updates of the WHOIS information relating to newly registered domain names. To achieve this, Verio devised an automated software program, or robot, which each day would submit multiple successive WHOIS queries through the port 43 accesses of various registrars. Upon acquiring the WHOIS information of new registrants, Verio would send them marketing solicitations by email, telemarketing and direct mail. ...

[Register objected. When Verio refused to stop marketing to Register's registrants, Register sued.]

DISCUSSION ...

(b) ***Verio's assent to Register's contract terms ...***

Verio contends that it nonetheless never became contractually bound to the conditions imposed by Register's restrictive legend because, in the case of each query Verio made, the legend did not appear until after Verio had submitted the query and received the WHOIS data. Accordingly, Verio contends that in no instance did it receive legally enforceable notice of the conditions Register intended to impose. Verio therefore argues it should not be deemed to have taken WHOIS data from Register's systems subject to Register's conditions.

Verio's argument might well be persuasive if its queries addressed to Register's computers had been sporadic and infrequent. If Verio had submitted only one query, or even if it had submitted only a few sporadic queries, that would give considerable force to its contention that it obtained the WHOIS data without being conscious that Register intended to impose conditions, and without being deemed to have accepted Register's conditions. But Verio was daily submitting numerous queries, each of which resulted in its receiving notice of the terms Register exacted. Furthermore, Verio admits that it knew perfectly well what terms Register demanded. Verio's argument fails.

The situation might be compared to one in which plaintiff P maintains a roadside fruit stand displaying bins of apples. A visitor, defendant D, takes an apple and bites into it. As D turns to leave, D sees a sign, visible only as one turns to exit, which says "Apples — 50 cents apiece." D does not pay for the apple. D believes he has no obligation to pay because he had no notice when he bit into the apple that 50 cents was expected in return. D's view is that he never agreed to pay for the apple. Thereafter, each day, several times a day, D revisits the stand, takes an apple, and eats it. D never leaves money.

P sues D in contract for the price of the apples taken. D defends on the ground that on no occasion did he see P's price notice until after he had bitten into the

apples. D may well prevail as to the first apple taken. D had no reason to understand upon taking it that P was demanding the payment. In our view, however, D cannot continue on a daily basis to take apples for free, knowing full well that P is offering them only in exchange for 50 cents in compensation, merely because the sign demanding payment is so placed that on each occasion D does not see it until he has bitten into the apple.

Verio's circumstance is effectively the same. Each day Verio repeatedly enters Register's computers and takes that day's new WHOIS data. Each day upon receiving the requested data, Verio receives Register's notice of the terms on which it makes the data available — that the data not be used for mass solicitation via direct mail, email, or telephone. Verio acknowledges that it continued drawing the data from Register's computers with full knowledge that Register offered access subject to these restrictions. Verio is no more free to take Register's data without being bound by the terms on which Register offers it, than D was free, in the example, once he became aware of the terms of P's offer, to take P's apples without obligation to pay the 50 cent price at which P offered them.

Verio seeks support for its position from cases that have dealt with the formation of contracts on the Internet. An excellent example, although decided subsequent to the submission of this case, is *Specht v. Netscape Communications Corp.*, 306 F.3d 17 (2d Cir. 2002). The dispute was whether users of Netscape's software, who downloaded it from Netscape's web site, were bound by an agreement to arbitrate disputes with Netscape, where Netscape had posted the terms of its offer of the software (including the obligation to arbitrate disputes) on the web site from which they downloaded the software. We ruled against Netscape and in favor of the users of its software because the users would not have seen the terms Netscape exacted without scrolling down their computer screens, and there was no reason for them to do so. The evidence did not demonstrate that one who had downloaded Netscape's software had necessarily seen the terms of its offer.

Verio, however, cannot avail itself of the reasoning of *Specht.* In *Specht,* the users in whose favor we decided visited Netscape's web site one time to download its software. Netscape's posting of its terms did not compel the conclusion that its downloaders took the software subject to those terms because there was no way to determine that any downloader had seen the terms of the offer. There was no basis for imputing to the downloaders of Netscape's software knowledge of the terms on which the software was offered. This case is crucially different. Verio visited Register's computers daily to access WHOIS data and each day saw the terms of Register's offer; Verio admitted that, in entering Register's computers to get the data, it was fully aware of the terms on which Register offered the access.

Verio's next argument is that it was not bound by Register's terms because it rejected them. Even assuming Register is entitled to demand compliance with its terms in exchange for Verio's entry into its systems to take WHOIS data, and even acknowledging that Verio was fully aware of Register's terms, Verio contends that it still is not bound by Register's terms because it did not agree to be bound. In support of its claim, Verio cites a district court case from the Central District of California, *Ticketmaster Corp. v. Tickets.com, Inc.*, No. CV99-7654, 2000 WL 1887522 (C.D. Cal. Aug. 10, 2000), in which the court rejected Ticketmaster's application for a preliminary injunction to enforce posted terms of use of data available on its website against a regular user. Noting that the user of Ticketmaster's web site is not required to check an "I agree" box before proceeding, the court con-

cluded that there was insufficient proof of agreement to support a preliminary injunction. ...

There is a crucial difference between the circumstances of *Specht,* where we declined to enforce Netscape's specified terms against a user of its software because of inadequate evidence that the user had seen the terms when downloading the software, and those of *Ticketmaster,* where the taker of information from Ticketmaster's site knew full well the terms on which the information was offered but was not offered an icon marked, "I agree," on which to click. Under the circumstances of *Ticketmaster,* we see no reason why the enforceability of the offeror's terms should depend on whether the taker states (or clicks), "I agree."

We recognize that contract offers on the Internet often require the offeree to click on an "I agree" icon. And no doubt, in many circumstances, such a statement of agreement by the offeree is essential to the formation of a contract. But not in all circumstances. While new commerce on the Internet has exposed courts to many new situations, it has not fundamentally changed the principles of contract. It is standard contract doctrine that when a benefit is offered subject to stated conditions, and the offeree makes a decision to take the benefit with knowledge of the terms of the offer, the taking constitutes an acceptance of the terms, which accordingly become binding on the offeree. *See, e.g.,* Restatement (Second) of Contracts § 69(1)(a) (1981) ("Silence and inaction operate as an acceptance ... where an offeree takes the benefit of offered services with reasonable opportunity to reject them and reason to know that they were offered with the expectation of compensation."); *Markstein Bros. Millinery Co. v. J.A. White & Co.*, 151 Ark. 1, 235 S.W. 39 (1921) (buyer of hats was bound to pay for hats when buyer failed to return them to seller within five days of inspection as seller requested in clear and obvious notice statement).

Returning to the apple stand, the visitor, who sees apples offered for 50 cents apiece and takes an apple, owes 50 cents, regardless whether he did or did not say, "I agree." The choice offered in such circumstances is to take the apple on the known terms of the offer or not to take the apple. As we see it, the defendant in *Ticketmaster* and Verio in this case had a similar choice. Each was offered access to information subject to terms of which they were well aware. Their choice was either to accept the offer of contract, taking the information subject to the terms of the offer, or, if the terms were not acceptable, to decline to take the benefits.

We find that the district court was within its discretion in concluding that Register showed likelihood of success on the merits of its contract claim.

C. Transfer Formalities

Rules about transferring property are created by law. There are only certain ways people can rearrange property relations. Some rearrangements happen even if the people involved don't want them, and some don't happen even if the people involved do want them. Knowing the rules is a way to understand which transfers work and why.

There are several methods of transferring property. The key ***voluntary*** methods are ***gifts***, ***sales***, and ***transfers at death***, which can be divided into transfers by ***will*** (also known as transfer by devise) and transfers by operation of law because of the decedent's ***intestacy*** (dying without a will). Although most litigated transfers involve sales, it is useful to study the others in order to appreciate the significance

of possession to ownership. Relatedly, gift law highlights that some problems in contract law arise only out of executory promises: completed promises involving property will often be valid as gifts, even if they lacked consideration. There are also various transfers ***by operation of law*** in which the legal system itself changes ownership without worrying about the transferors intent: in addition to intestacy, other familiar forms include eminent domain, bankruptcy, and the execution of judgments.

This section is about the ***formalities*** required to make a property transfer effective. These are the elements without which the transfer of legal rights does not happen. Delivery is typically effective to transfer ownership of personal property because possession is so central to how personal property is owned and used. For other forms of property, however, it is more common to use a written instrument, or ***deed***. For real property, the Statute of Frauds generally requires the use of a writing. There is a bit of a historical irony here. In 1250, to transfer ownership of land, the grantor and grantee would physically go to the land. The grantor would physically (or perhaps metaphysically) put the grantee in possession by handing over a clod of dirt. The grantee would swear homage to the grantor, and the grantor would swear to defend the grantee's title. This was a public ceremony, performed in front of witnesses who could later be called on to recall what had happened if necessary. In contrast, written conveyances—called "charters"—were treated with skepticism; they were considered an inferior form of evidence because of the risk of forgery. In the seven and a half centuries since, this attitude has completely flipped.

For many kinds of intellectual and intangible property, there is no meaningful way to transfer possession, so using a writing is the only available way of making clear that ownership has changed hands. Think about a corporate merger: thousands of pages of deal documents are designed to ensure that exactly the right financial assets change hands in exactly the right way.

LON L. FULLER
CONSIDERATION AND FORM
41 COLUM. L. REV. 799 (1941)

§ 2. *The Evidentiary Function.*—The most obvious function of a legal formality is, to use Austin's words, that of providing "evidence of the existence and purport of the contract, in case of controversy." The need for evidentiary security may be satisfied in a variety of ways: by requiring a writing, or attestation, or the certification of a notary. It may even be satisfied, to some extent, by such a device as the Roman *stipulatio*, which compelled an oral spelling out of the promise in a manner sufficiently ceremonious to impress its terms on participants and possible bystanders.

§ 3. *The Cautionary Function.*—A formality may also perform a cautionary or deterrent function by acting as a check against inconsiderate action. The seal in its original form fulfilled this purpose remarkably well. The affixing and impressing of a wax wafer-symbol in the popular mind of legalism and weightiness-was an excellent device for inducing the circumspective frame of mind appropriate in one pledging his future. To a less extent any requirement of a writing, of course, serves the same purpose, as do requirements of attestation, notarization, etc.

§ 4. *The Channeling Function.*—... That a legal formality may perform a function not yet described can be shown by the seal. The seal not only insures a satis-

factory memorial of the promise and induces deliberation in the making of it. It serves also to mark or signalize the enforceable promise; it furnishes a simple and external test of enforceability. ... The thing which characterizes the law of contracts and conveyances is that in this field forms are deliberately used, and are intended to be so used, by the parties whose acts are to be judged by the law. To the business man who wishes to make his own or another's promise binding, the seal was at common law available as a device for the accomplishment of his objective. In this aspect form offers a legal framework into which the party may fit his actions, or, to change the figure, it offers channels for the legally effective expression of intention.

JOHN H. LANGBEIN
SUBSTANTIAL COMPLIANCE WITH THE WILLS ACT
88 HARV.. L. REV. 489 (1975)

4. *The Protective Function.*—Courts have traditionally attributed to the Wills Act the object "of protecting the testator against imposition at the time of execution." The requirement that attestation be made in the presence of the testator is meant "to prevent the substitution of a surreptitious will." Another common protective requirement is the rule that the witnesses should be disinterested, hence not motivated to coerce or deceive the testator.

UNIFORM COMMERCIAL CODE [STATUTE OF FRAUDS]

§ 2-201 – *Formal Requirements; Statute of Frauds.*

(1) Except as otherwise provided in this section a contract for the sale of goods for the price of $500 or more is not enforceable by way of action or defense unless there is some writing sufficient to indicate that a contract for sale has been made between the parties and signed by the party against whom enforcement is sought or by his authorized agent or broker. A writing is not insufficient because it omits or incorrectly states a term agreed upon but the contract is not enforceable under this paragraph beyond the quantity of goods shown in such writing.

(2) Between merchants if within a reasonable time a writing in confirmation of the contract and sufficient against the sender is received and the party receiving it has reason to know its contents, it satisfies the requirements of subsection (1) against such party unless written notice of objection to its contents is given within 10 days after it is received.

(3) A contract which does not satisfy the requirements of subsection (1) but which is valid in other respects is enforceable

(a) if the goods are to be specially manufactured for the buyer and are not suitable for sale to others in the ordinary course of the seller's business and the seller, before notice of repudiation is received and under circumstances which reasonably indicate that the goods are for the buyer, has made either a substantial beginning of their manufacture or commitments for their procurement; or

(b) if the party against whom enforcement is sought admits in his pleading, testimony or otherwise in court that a contract for sale was made, but the contract is not enforceable under this provision beyond the quantity of goods admitted; or

(c) with respect to goods for which payment has been made and accepted or which have been received and accepted.

NOTES

1. Why $500? Should that be higher or lower? Why not include contracts for services too?
2. Look at the exceptions in subsections (2) and (3). Do they fatally undermine the point of a statute of frauds? What would Fuller and Langbein say?

INDIANA CODE [STATUTE OF FRAUDS]

§ 32-21-1-1 – *Requirement of written agreement; agreements or promises covered*

(a) This section does not apply to a lease for a term of not more than three (3) years.

(b) A person may not bring any of the following actions unless the promise, contract, or agreement on which the action is based, or a memorandum or note describing the promise, contract, or agreement on which the action is based, is in writing and signed by the party against whom the action is brought or by the party's authorized agent: ...

(4) An action involving any contract for the sale of land.

(5) An action involving any agreement that is not to be performed within one (1) year from the making of the agreement.

§ 32-21-1-13 – *Conveyance of land; written deed required*

Except for a bona fide lease for a term not exceeding three (3) years, a conveyance of land or of any interest in land shall be made by a deed that is:

(1) written; and

(2) subscribed, sealed, and acknowledged by the grantor ... or by the grantor's attorney.

NOTES

1. What is the difference between these two sections? Why are both necessary?
2. How well does the statute of frauds serve the various functions identified by Fuller and Langbein?

LOUGHRAN V. KUMMER

146 A. 534 (Pa. 1929)

Kephart, Justice:

Appellee, a bachelor 67 years of age, conveyed, for $1, land in Pittsburgh to Mrs. Kummer, appellant, who was one of his tenants. A bill was filed to set aside this deed; the grounds laid were confidential relationship, undue influence, and impaired mentality. Inasmuch as the facts must again be considered, we will mention only such as raise the legal question on which the case was decided; we venture no opinion on the other facts.

The court below found from the evidence that a deed absolute on its face had been executed, acknowledged, and delivered to appellant by appellee, on condition that it should not be recorded until the latter's death; that undoubtedly in his mind this meant that the deed was not to take effect until after his death; and that he, demanding the return of the deed within a very few days after the delivery,

thus revoked it and with that revocation revoked the gift. Appellant deceived appellee when she stated the deed had been destroyed. The excuse given was appellee was worried and she wanted to ease his mind by making him believe that it had been destroyed. ...

The question we are asked to consider is whether a deed absolute on its face, acknowledged, executed, and delivered under circumstances as here indicated, vested such title in the grantee as could be revoked for the above reasons. It amounts in substance to this, that the grantor said the deed should not be recorded until after his death, and the grantee in accepting the deed took it on that condition. The evidence on which this finding was based was all oral, and the scrivener and defendant denied any such condition was imposed when the deed was delivered. All control over the deed was relinquished when it was handed appellant. The presumption must be that at that time it was the intention to pass title. 'The general principle of law is that the formal act of signing, sealing and delivering is the consummation of the deed, and it lies with the grantor to prove clearly that appearances are not consistent with truth. The presumption stands against him, and the burden is on him to destroy it by clear and positive proof that there was no delivery and that it was so understood at the time. ... Where we have, as here, a deed, absolute and complete in itself, attacked as being in fact otherwise intended, ... there is a further presumption that the title is in conformity with the deed, and it should not be dislodged except by clear, precise, convincing and satisfactory evidence to the contrary.' *Cragin's Estate*, 117 A. 445 (Pa. 1922).

The gift here was executed, and that defendant was not to record it was not of the slightest consequence when viewed as against these major actions, delivery and passing of title. It was merely a promise the keeping of which lay in good faith, the breach of which entailed no legal consequences. To have effected the grantor's purpose, the intervention of a third party was absolutely essential. There are circumstances where acknowledgment, together with physical possession of the deed in the grantee, does not conclusively establish an intention to deliver, and the presumption arising from signing, sealing, and acknowledging, accompanied by manual possession of the deed by the grantee, is not irrebuttable, but this presumption can be overcome only by evidence that no delivery was in fact intended and none made. Such evidence is not present in this case. Here the grantor by his own testimony intended the grantee to get the land. The only question was when it was to take effect.

Here is one of the instances in which the law fails to give effect to the honest intention of the parties, for the reason that they have not adopted the proper legal means of accomplishing their object. Therefore the legal effect of such delivery is not altered by the fact that both parties suppose the deed will not take effect until recorded, and that it may be revoked at any time before record, or by contemporaneous agreements looking to the reconveyance of the property to the grantor or to the third party upon the happening of certain contingent events or the nonperformance of certain conditions.

The reason for these rules is obvious. It is quite possible to prove in most deliveries that some parol injunction was attached to the formal delivery of the deed; if they are to be given the effect her contended, there would be no safety in accepting a deed under most circumstances. It opens the door to the fabrication of evidence that would inevitably be appalling and go far toward violating the security of written instruments. We have so held in matters of less import than the conveyance of land. The rule must not be relaxed as to realty. Such conveyances are vastly more

important, as they involve instruments of title and ownership which are used as a means of extending credit. Title to land ought not to be exposed to the peril of successful attack except where the right is clear and undoubted, and whatever may be our desire to recognize circumstances argued as unfortunate, we cannot go to the extent of overthrowing principles of law governing conveyances of real estate that have stood the test of ages.

In *Cragin's Estate*, the deeds were in a tin box for more than 23 years in an envelope indorsed with the words: 'To be recorded upon Mrs. Cragin's death, if before me.' The deed was in grantee's possession, and it was urged the delivery was conditional. We said that indorsement may have been placed on the envelope for other reasons than to defer the transfer of title. In the present case it was evident appellee did not want his relatives to learn of the conveyance. Recording would be necessary to pass a title examiner's inspection, but nonrecording did not prevent the title from passing. It has been quite generally held that an oral understanding on the delivery of a deed that it should not be recorded will not affect the absolute character of the conveyance if free of other conditions. n agreement to deliver a deed in escrow to the person in whose favor it is made, and who is likewise a party to it, will not make the delivery conditional. If delivered under such an agreement, it will be deemed an absolute delivery and a consummation of the execution of the deed. ...

NOTES

1. The old phrase is that a deed was effective when it was "signed, sealed, and delivered." But the seal is obsolete, so the principal elements are that it be a sufficient writing, that it be signed, and that it be delivered. In a famous passage of his landmark 17th-century treatise, *Institutes of the Lawes of England*, Edward Coke wrote, "As a deed may be delivered to a party without words, so may a deed be delivered by words without any act of delivery." That sounds paradoxical, but Coke continued, "as if the writing sealed lies upon the table, and the [grantor] says to the [grantee], 'Go and take up that writing, it is sufficient for you;' or 'it will serve your turn;' or 'Take it as my deed;' or the like words; either is a sufficient delivery." Is that better?
2. There are at least two ways to do delivery "right." One is to sign and hand over a deed at closing, when all of the necessary parties are in the same room and can execute all of the appropriate documents effectively simultaneously. Another is to use an escrow: a third party who receives custody of the signed deed along with instructions to deliver it to the grantee when appropriate events have taken place. What if the escrow agent disregards her instructions and hands over the deed early? Can a grantor who is concerned the transaction will fall through demand the deed back from the escrow agent?
3. A valid gift requires the *intent* to make a gift, *delivery* of the gift, and *acceptance* by the recipient. The common law required manual delivery of personal property for a valid gift unless the object was too big to move. See, e.g., *Newman v. Bost*, 20 S.E. 848 (N.C. 1898) (symbolic delivery insufficient where objects were small items that could easily have been physically delivered, even though would-be donor was ill in bed). If the object was too big to move, substitutes for physical delivery were acceptable. Keys are a classic example: at common law, handing over car keys was considered a "constructive" or "symbolic" delivery of the car. The keys symbolized the car (symbolic delivery) and provided the means for exercising dominion and control over it

(constructive delivery). If delivery is a kind of formality, how well does it serve the various functions identified by Fuller and Langbein?

4. Governments also often regulate transfer formalities for specific types of property. Title registries are a good example. Today, because all states require car owners to register the title to their cars, many states require that a transfer of a car (whether by gift or by sale) is not complete unless the donor also hands over the title documents. Why would the law require delivery of the title documents? What happens when someone who doesn't know this rule hands over only the keys, and then a year later changes her mind and demands the car back? (You should see here how a title system can both make it easier to determine who owns property and easier for legally unsophisticated people to make significant mistakes.)

D. Good Faith Purchase for Value

UNIFORM COMMERCIAL CODE [GOOD FAITH PURCHASE]

§ 2-403. Power to transfer; good faith purchase of goods; "entrusting"

(1) A purchaser of goods acquires all title which his transferor had or had power to transfer except that a purchaser of a limited interest acquires rights only to the extent of the interest purchased. A person with voidable title has power to transfer a good title to a good faith purchaser for value. When goods have been delivered under a transaction of purchase the purchaser has such power even though

   (a) The transferor was deceived as to the identity of the purchaser, or

   (b) The delivery was in exchange for a check which is later dishonored, or

   (c) It was agreed that the transaction was to be a "cash sale," or

   (d) The delivery was procured through fraud punishable as larcenous under the criminal law.

(2) Any entrusting of possession of goods to a merchant who deals in goods of that kind gives him power to transfer all rights of the entruster to a buyer in ordinary course of business.

(3) "Entrusting" includes any delivery and any acquiescence in retention of possession regardless of any condition expressed between the parties to the delivery or acquiescence and regardless of whether the procurement of the entrusting or the possessor's disposition of the goods have been such as to be larcenous under the criminal law.

KOTIS V. NOWLIN JEWELRY, INC.

844 S.W.2d 920 (Tex. App. 1992)

Draughn, Justice:

Eddie Kotis appeals from a judgment declaring appellee, Nowlin Jewelry, Inc., the sole owner of a Rolex watch, and awarding appellee attorney's fees. Kotis raises fourteen points of error. We affirm.

On June 11, 1990, Steve Sitton acquired a gold ladies Rolex watch, President model, with a diamond bezel from Nowlin Jewelry by forging a check belonging to his brother and misrepresenting to Nowlin that he had his brother's authorization

for the purchase. The purchase price of the watch, and the amount of the forged check, was $9,438.50. The next day, Sitton telephoned Eddie Kotis, the owner of a used car dealership, and asked Kotis if he was interested in buying a Rolex watch. Kotis indicated interest and Sitton came to the car lot Kotis purchased the watch for $3,550.00. Kotis also called Nowlin's Jewelry that same day and spoke with Cherie Nowlin.

Ms. Nowlin told Kotis that Sitton had purchased the watch the day before. Ms. Nowlin testified that Kotis would not immediately identify himself. Because she did not have the payment information available, Ms. Nowlin asked if she could call him back. Kotis then gave his name and number. Ms. Nowlin testified that she called Kotis and told him the amount of the check and that it had not yet cleared. Kotis told Ms. Nowlin that he did not have the watch and that he did not want the watch. Ms. Nowlin also testified that Kotis would not tell her how much Sitton was asking for the watch.

John Nowlin, the president of Nowlin's Jewelry, testified that, after this call from Kotis, Nowlin's bookkeeper began attempting to confirm whether the check had cleared. When they learned the check would not be honored by the bank, Nowlin called Kotis, but Kotis refused to talk to Nowlin. Kotis referred Nowlin to his attorney. On June 25, 1990, Kotis' attorney called Nowlin and suggested that Nowlin hire an attorney and allegedly indicated that Nowlin could buy the watch back from Kotis. Nowlin refused to repurchase the watch.

After Sitton was indicted for forgery and theft, the district court ordered Nowlin's Jewelry to hold the watch until there was an adjudication of the ownership of the watch. Nowlin then filed suit seeking a declaratory judgment that Nowlin was the sole owner of the watch. Kotis filed a counterclaim for a declaration that Kotis was a good faith purchaser of the watch and was entitled to possession and title of the watch. After a bench trial, the trial court rendered judgment declaring Nowlin the sole owner of the watch. The trial court also filed Findings of Fact and Conclusions of Law.

In point of error one, Kotis claims the trial court erred in concluding that Sitton did not receive the watch through a transaction of purchase with Nowlin, within the meaning of TEX. BUS. & COM. CODE ANN. § 2.403(a). Where a party challenges a trial court's conclusions of law, we may sustain the judgment on any legal theory supported by the evidence. Incorrect conclusions of law will not require reversal if the controlling findings of facts will support a correct legal theory.

Kotis contends there is evidence that the watch is a "good" under the UCC, there was a voluntary transfer of the watch, and there was physical delivery of the watch. Thus, Kotis maintains that the transaction between Sitton and Nowlin was a transaction of purchase such that Sitton acquired the ability to transfer good title to a good faith purchaser under § 2.403 [which was identical in relevant part to the UCC excerpt quoted above]. ...

Neither the code nor case law defines the phrase "transaction of purchase." "Purchase" is defined by the code as a "taking by sale, discount, negotiation, mortgage, pledge, lien, issue or reissue, gift or any other voluntary transaction creating an interest in property." TEX. BUS. & COM. CODE ANN. § 1.201(32). Thus, only voluntary transactions can constitute transactions of purchase.

Having found no Texas case law concerning what constitutes a transaction of purchase under § 2.403(a), we have looked to case law from other states. Based on the code definition of a purchase as a voluntary transaction, these cases reason that a thief who wrongfully takes the goods against the will of the owner is not a

purchaser. *See Suburban Motors, Inc. v. State Farm Mut. Automobile Ins. Co.*, *Charles Evans BMW, Inc. v. Williams* 395 S.E.2d 650, 651-52 (Ga. Ct. App. 1990); *Inmi-Etti v. Aluisi*, 492 A.2d 917 (Md. Ct. App. 1985). On the other hand, a swindler who fraudulently induces the victim to deliver the goods voluntarily is a purchaser under the code.

In this case, Nowlin's Jewelry voluntarily delivered the watch to Sitton in return for payment by check that was later discovered to be forged. Sitton did not obtain the watch against the will of the owner. Rather, Sitton fraudulently induced Nowlin's Jewelry to deliver the watch voluntarily. Thus, we agree with appellant that the trial court erred in concluding that Sitton did not receive the watch through a transaction of purchase under § 2.403(a). We sustain point of error one.

In point of error two, Kotis contends the trial court erred in concluding that, at the time Sitton sold the watch to Kotis, Sitton did not have at least voidable title to the watch. In point of error nine, Kotis challenges the trial court's conclusion that Nowlin's Jewelry had legal and equitable title at all times relevant to the lawsuit. The lack of Texas case law addressing such issues under the code again requires us to look to case law from other states to assist in our analysis.

In *Suburban Motors, Inc. v. State Farm Mut. Automobile Ins. Co.,* 268 Cal. Rptr. 16, 18 (Cal. Ct. App. 1990); the California court noted that § 2.403 provides for the creation of voidable title where there is a voluntary transfer of goods. Section 2.403(a)(1)-(4) set forth the types of voluntary transactions that can give the purchaser voidable title. Where goods are stolen such that there is no voluntary transfer, only void title results. Subsection (4) provides that a purchaser can obtain voidable title to the goods even if "delivery was procured through fraud punishable as larcenous under the criminal law." This subsection applies to cases involving acts fraudulent to the seller such as where the seller delivers the goods in return for a forged check. Although Sitton paid Nowlin's Jewelry with a forged check, he obtained possession of the watch through a voluntary transaction of purchase and received voidable, rather than void, title to the watch. Thus, the trial court erred in concluding that Sitton received no title to the watch and in concluding that Nowlin's retained title at all relevant times. We sustain points of error two and nine.

In point of error three, Kotis claims the trial court erred in concluding that Kotis did not give sufficient value for the watch to receive protection under § 2.403, that Kotis did not take good title to the watch as a good faith purchaser, that Kotis did not receive good title to the watch, and that Kotis is not entitled to the watch under § 2.403. In points of error four through eight, Kotis challenges the trial court's findings regarding his good faith, his honesty in fact, and his actual belief, and the reasonableness of the belief, that the watch had been received unlawfully.

Under § 2.403(a), a transferor with voidable title can transfer good title to a good faith purchaser. Good faith means "honesty in fact in the conduct or transaction concerned." TEX. BUS. & COM. CODE ANN. § 1.201(19). The test for good faith is the actual belief of the party and not the reasonableness of that belief.

Kotis was a dealer in used cars and testified that he had bought several cars from Sitton in the past and had no reason not to trust Sitton. He also testified that on June 12, 1990, Sitton called and asked Kotis if he was interested in buying a Ladies Rolex. Once Kotis indicated his interest in the watch, Sitton came to Kotis's place of business. According to Kotis, Sitton said that he had received $18,000.00 upon the sale of his house and that he had used this to purchase the watch for his girlfriend several months before. Kotis paid $3,550.00 for the watch. Kotis further testified that he then spoke to a friend, Gary Neal Martin, who also knew Sitton.

Martin sagely advised Kotis to contact Nowlin's to check whether Sitton had financed the watch. Kotis testified that he called Nowlin's after buying the watch.

Cherie Nowlin testified that she received a phone call from Kotis on June 12, 1990, although Kotis did not immediately identify himself. Kotis asked if Nowlin's had sold a gold President model Rolex watch with a diamond bezel about a month before. When asked, Kotis told Ms. Nowlin that Sitton had come to Kotis' car lot and was trying to sell the watch. Ms. Nowlin testified that Kotis told her he did not want the watch because he already owned a Rolex. Ms. Nowlin told Kotis that Sitton had purchased the watch the day before. Kotis asked about the method of payment. Because Ms. Nowlin did not know, she agreed to check and call Kotis back. She called Kotis back and advised him that Sitton had paid for the watch with a check that had not yet cleared. When Ms. Nowlin asked if Kotis had the watch, Kotis said no and would not tell her how much Sitton was asking for the watch. Ms. Nowlin did advise Kotis of the amount of the check.

After these calls, the owner of Nowlin's asked his bookkeeper to call the bank regarding Sitton's check. They learned on June 15, 1990 that the check would be dishonored. John Nowlin called Kotis the next day and advised him about the dishonored check. Kotis refused to talk to Nowlin and told Nowlin to contact his attorney. Nowlin also testified that a reasonable amount to pay for a Ladies President Rolex watch with a diamond bezel in mint condition was $7,000.00-$8,000.00. Nowlin maintained that $3,500.00 was an exorbitantly low price for a watch like this.

The trier of fact is the sole judge of the credibility of the witnesses and the weight to be given their testimony. Kotis testified that he lied when he spoke with Cherie Nowlin and that he had already purchased the watch before he learned that Sitton's story was false. The judge, as the trier of fact, may not have believed Kotis when he said that he had already purchased the watch. If the judge disbelieved this part of Kotis' testimony, other facts tend to show that Kotis did not believe the transaction was lawful. For example, when Kotis spoke with Nowlin's, he initially refused to identify himself, he said that he did not have the watch and that he did not want the watch, he refused to divulge Sitton's asking price, and he later refused to talk with Nowlin and advised Nowlin to contact Kotis' attorney. Thus, there is evidence supporting the trial court's finding that Kotis did not act in good faith.

There are sufficient facts to uphold the trial court's findings even if the judge had accepted as true Kotis' testimony that, despite his statements to Nowlin's, he had already purchased the watch when he called Nowlin's. The testimony indicated that Kotis was familiar with the price of Rolex watches and that $3,550.00 was an extremely low price for a mint condition watch of this type. An unreasonably low price is evidence the buyer knows the goods are stolen. Although the test is what Kotis actually believed, we agree with appellee that we need not let this standard sanction willful disregard of suspicious facts that would lead a reasonable person to believe the transaction was unlawful. Thus, we find sufficient evidence to uphold the trial court's findings regarding Kotis' lack of status as a good faith purchaser. We overrule points of error three through eight. ...

We affirm the trial court's judgment.

NOTES

1. The common-law baseline is *nemo dat quod non habet*: no man can give what he does not have. If I "give" you a car I don't own, you don't own it either. If I sell you a tract of land encumbered by a mortgage and an easement, you receive only as much as I owned, so you take the land subject to the

mortgage and the easement. This *nemo dat* baseline is the source of the maxim that a thief cannot give good title. So if Sitton had held up Nowlin's at gunpoint, how would the case have come out, and on what reasoning?

2. UCC § 2-403(1), as applied in *Kotis*, distinguishes the thief's "void" title from merely "voidable" title: the quality of title obtained by the buyer in a transaction that is for some reason defective. If the seller in that defective transaction discovers the problem, she has a right to unwind the transaction (and get her stuff back). But until she does, the buyer has the power to convey not just his own, voidable title, but something even better. A good-faith purchaser for value receives good title, *even as against the original seller.* Her right to unwind the transaction has been cut off. This is a harsh way to treat an innocent victim of fraud or mistake. Why would property law do something like that?
3. How did the parties get into this mess? Obviously Sitton is most to blame, but is there anything Kotis or Nowlin could have done? Who is left holding the bag and why? Is there anything Kotis can do to recover his $3,550.00?
4. UCC § 2-403 provides for two tests that the buyer must meet to be protected (in addition to the threshold question of whether his seller had voidable title): he must act in good faith and he must give "value." Which of these tripped up Kotis? And what is the reason for not protecting donees along with buyers?

HARDING V. JA LAUR

315 A.2d 132 (Md. Ct. Spec. App. 1974)

Gilbert, Judge: ...

The bill alleged that a deed had been obtained from the appellant through fraud practiced upon her by the agent of Ja Laur Corporation. The bill further averred that the paper upon which the appellant had affixed her signature was "falsely and fraudulently attached to the first page of a deed identified as the same deed" through which the appellee, Ja Laur Corporation, and its assigns, the other appellees, claim title. ...

There is no dispute that the appellant signed some type of paper. Her claim is not that her signature was forged in the normal sense, i.e., someone copied or wrote it, but rather that the forgery is the result of an alteration. Mrs. Harding alleges that at the time that she signed a blank paper she was told that her signature was necessary in order to straighten out a boundary line. She represents that she did not know that she was conveying away her interest in and to a certain 1517 acres of land in Montgomery County.

The parcel of land that was conveyed by the allegedly forged deed is contiguous to a large tract of real estate in which Ja Laur and others had "a substantial interest." It appears from the bill that Mrs. Harding's land provided the access from the larger tract to a public road, so that its value to the appellees is obvious. Mrs. Harding excuses herself for signing the "blank paper" by averring that she did so at the instigation of an attorney, an agent of Ja Laur, who had "been a friend of her deceased husband, and ... represented her deceased husband in prior business and legal matters, and that under [the] circumstances [she] did place her complete trust and reliance in the representations made to her ..." by the attorney. The "blank paper" was signed "on or about April 2, 1970." Mrs. Harding states that she did not learn of the fraud until the "summer of 1972." At that time an audit, by the

Internal Revenue Service, of her deceased husband's business revealed the deed to Ja Laur, and its subsequent conveyance to the other appellees.

In *Smith v. State*, 256 A.2d 357, 360 (1970), we said that:

> Forgery has been defined as a false making or material alteration, with intent to defraud, of any writing which, if genuine, might apparently be of legal efficacy or the foundation of a legal liability. More succinctly, forgery is the fraudulent making of a false writing having apparent legal significance. It is thus clear that one of the essential elements of forgery is a writing in such form as to be apparently of some legal efficacy and hence capable of defrauding or deceiving.

Perkins, *Criminal Law* ch. 4, § 8 (2d ed. 1969) states, at 351:

> A material alteration may be in the form of (1) an addition to the writing, (2) a substitution of something different in the place of what originally appeared, or (3) the removal of part of the original. The removal may be by erasure or in some other manner, such as by cutting off a qualifying clause appearing after the signature.

A multitude of cases hold that forgery includes the alteration of or addition to any instrument in order to defraud. That a deed may be the subject of a forgery is beyond question.

The Bill of Complaint alleges that the signature of Mrs. Harding was obtained through fraud. More important, however, to the issue is whether or not the bill alleges forgery. In our view the charge that appellant's signature was written upon a paper, which paper was thereafter unbeknown to her made a part of a deed, if true, demonstrates that there has been a material alteration and hence a forgery. ...

We turn now to the discussion of whether *vel non* the demurrers of Macro Housing, Inc. and Montgomery County, the other appellees, should have been sustained. There was no allegation in the bill that their agent had perpetrated the fraud upon Mrs. Harding. If they are to be held in the case, it must be on the basis that they are not *bona fide* purchasers without notice. The title of a *bona fide* purchaser, without notice, is not vitiated even though a fraud was perpetrated by his vendor upon a prior title holder. A deed obtained through fraud, deceit or trickery is voidable as between the parties thereto, but not as to a *bona fide* purchaser. A forged deed, on the other hand, is void *ab initio*. ...

[T]he common law rule that a forger can pass no better title than he has is in full force and effect in this State. A forger, having no title can pass none to his vendee. Consequently, there can be no *bona fide* holder of title under a forged deed. A forged deed, unlike one procured by fraud, deceit or trickery is void from its inception. The distinction between a deed obtained by fraud and one that has been forged is readily apparent. In a fraudulent deed an innocent purchaser is protected because the fraud practiced upon the signatory to such a deed is brought into play, at least in part, by some act or omission on the part of the person upon whom the fraud is perpetrated. He has helped in some degree to set into motion the very fraud about which he later complains. A forged deed, on the other hand, does not necessarily involve any action on the part of the person against whom the forgery is committed. So that if a person has two deeds presented to him, and he thinks he is signing one but in actuality, because of fraud, deceit or trickery he signs the other, a bona fide purchaser, without notice, is protected. On the other hand, if a person is presented with a deed, and he signs that deed but the deed is

thereafter altered e.g. through a change in the description or affixing the signature page to another deed, that is forgery and a subsequent purchaser takes no title.

In the instant case, the Bill of Complaint, for the reasons above stated, alleged a forgery of the deed by which Ja Laur took title from Mrs. Harding. This allegation, if true, renders that deed a nullity. Ja Laur could not have passed title to the other appellees, Macro Housing, Inc. and Montgomery County. Those two appellees would therefore have no title to the land of Mrs. Harding. ...

NOTES

1. What is the point of the distinction between forging a deed (sometimes called "fraud in the factum") and tricking someone into signing it ("fraud in the inducement")? As between the fraudster and the victim, is there a significant difference? What about once third parties get involved?
2. Mrs. Harding signs a blank piece of paper, which Ja Laur then staples to a deed. Forgery? What if she signs the same piece of paper *after* it is stapled to the deed? Do the policy reasons for distinguishing forgery from fraud provide a convincing reason to treat these cases differently?