Diamond, E. and Bates, S. “Law and order comes to cyberspace”, *Technological Review* (October 1995).

Law and Order Comes to Cyberspace
By Edwin Diamond and Stephen Bates

At the electronic frontier of computer networks, rules and regulations have been few. But as millions of settlers move into cyberspace, the new medium must accomodate the sometimes ill-suited legal restraints of civilization.

EDWIN DIAMOND is a journalist and director of the News Study Group at New York University. STEPHEN BATES, a writer and lawyer, is a senior fellow at the Annenberg Washington Program in Communications Policy Studies, a nonpartisan think tank. They are the authors of, among other books, The Spot: The Rise of Political Advertising on Television (MIT Press, 3d ed., 1992). Individually or jointly, they have written about the Internet for American Heritage, the New York Times, the Wall Street Journal, The Hill, and other publications. *Peter Hyman and Julie Ziegler, members of the News Study Group, provided research help for this article.*

Cyberenthusiasts sing the praises of the body electric, a global realm of freewheeling computer networks where speech is open and no restrictive rules apply. But because the Internet ("the Net") exists within societies that have long-standing traditions and laws, its rapid assimilation into the "real world" is provoking tensions and confrontations that are now being played out in the legal domain.

This spring, for example, the U.S. Senate passed the Communications Decency Act, authored by Sen. James Exon (D-Nebr.), a bill that would give the Federal Communications Commission the power to regulate "indecency" on the Internet. A number of state legislatures are considering similar legislation. Net enthusiasts and systems operators argue that the Exon bill and proposals like it are unconstitutional as well as unworkable: if a literary magazine put its contents online, for example, and included a short story with a four-letter word, the law could leave the editor liable for a $50,000 fine and six months in jail. Speaker Newt Gingrich, professed cyberspace enthusiast, also opposes Exon; the bill is now awaiting action in the House of Representatives. Following the Oklahoma City explosion, Sen. Diane Feinstein (D- Calif.) introduced a bill to crack down on bomb-making guides on the Internet, an understandable, if somewhat emotional, reaction to domestic terror acts. The Feinstein bill passed the Senate and is awaiting House consideration. Meanwhile, several states are considering bills to criminalize "online stalking"--repeatedly making cybercontact with an unwilling subject. Connecticut has enacted one into law.

Whatever the fate of these regulations, in the legislatures and in the courts, the concerns they reflect won't go away. Battles over the boundaries of online free speech have erupted with increasing frequency over the past year or so, as the Internet has grown in population and in public awareness. The Net is a breeding ground for all kinds of expression, some of it lyrical and wise, but some of it vile and hateful, all of it easily accessible to anyone who

logs on. Because freedom of expression is generally contested only when the speech is repugnant, the cases that have arisen tend to focus on the seamier side of the Net.

Indeed, a major factor driving such legislation is the prevalence of pornography in cyberspace. A Carnegie Mellon study found 68 commercial "adult" computer bulletin board systems (BBSs) located in 32 states with a repertory of, in the researchers' dry words, "450,620 pornographic images, animations, and text files which had been downloaded by consumers 6,432,297 times." Concerned by these findings and attempting to comply with Pennsylvania's obscenity laws, the university banished many Internet "newsgroups" that offered sexually explicit photographic images, movie clips, sounds, stories, and discussions, noting that Pittsburgh-area high schools had access to these newsgroups through the Carnegie Mellon system. Under fire for censorship, the university restored the text-only sex newsgroups, but not the ones carrying photographic images.

Five Difficult Issues

The Net has thus become a First Amendment battleground. The resolution of the ensuing legal battles--some of which are likely to reach the Supreme Court--will help shape the conduct and culture of computer communications in the decades ahead. These conflicts revolve around a few fundamental questions.

1. How far does the Constitution go in protecting repugnant or defamatory speech on the Net?

Earlier this year, University of Michigan undergraduate Jake Baker was arrested by FBI agents for posting to the alt.sex.stories newsgroup a violent narrative of rape and torture that used the real name of a female classmate for the victim. Baker subsequently e-mailed a friend that "just thinking about it [his fantasies] doesn't do the trick anymore. I need to do it." The university suspended him and a federal judge ordered him held without bail, charged with the federal crime of "transporting threatening material" across state lines.

Some civil liberties groups rushed to the student's defense, arguing that the Constitution guarantees freedom even for repugnant fantasies broadcast worldwide. In June, a federal judge in Detroit implicitly agreed, throwing out the case. While the university acted properly in disciplining the student for his behavior, the judge ruled, there was no cause for a criminal indictment.

The press critic A. J. Liebling once observed, "Freedom of the press is guaranteed only to those who own one." On the Internet, for better or worse, everybody "owns" a press. Baker did not have to send his grotesque tale to a series of kinky magazines until one finally accepted it for publication; he, like any other Internet user, could simply upload his word-processed file to alt.sex.stories, where no editor checks for spelling or grammar, let alone merit.

The young woman could still bring civil action against Baker for libel. When Penthouse published a piece of short fiction about the sexual adventures of a "Miss Wyoming" a few years ago, the real Miss Wyoming sued. Her case was thrown out because the piece was unambiguously fictional, but a Baker-like case, where the writer knows the subject, might reach a jury.

The Jake Bakers of the world, and their supporters, could also be stopped by gatekeepers, aka censors. Although Net boosters extol the new medium for providing the freest speech the world has ever known, more and more monitors have been showing up, like hall patrols in a rowdy high school. For example, some online services screen messages sent to public chat areas, often using software that scans for comedian George Carlin's seven dirty words. The moderators of some mailing lists and Usenet groups exclude materials that they deem inappropriate. And some exclusions can be downright aggressive: renegade users have

created software agents--"cancelbots"-- that delete other users' public Usenet messages by forging a cancel command that seems to originate with the author of the original message.

But when public officials try to restrict information, such as in public schools, state universities, or government offices, they are potentially infringing on the First Amendment. We therefore foresee the day when a court might well order a state university to restore students' access to the alt.sex hierarchy. Restrictions of online speech, including hate speech, would also be subject to protection under the Constitution. In the past, the courts have established a "public forum doctrine" guaranteeing the right to speak in public parks and streets; some states have extended the doctrine to cover large private gathering places, such as shopping malls. Some courts will no doubt rule that the idea of a public forum applies to privately owned computer bulletin boards as well.

Litigation isn't the only way to resolve conflicts over free speech on computer networks. America Online general counsel Ellen Kirsch recently lit a small candle of good sense in the gathering cyber gloom. A lawyer from a major midwestern firm complained to America Online about postings that, he wrote, "defamed" the product of one of his clients. Kirsch responded by sending the lawyer an AOL starter kit with three hours of free time and urged him to put up his own postings defending the product. Her move was in the tradition of Supreme Court Justice Louis Brandeis, who believed that the solution to "bad speech" was not censorship but more speech.

Yet system operators may still be caught in the middle. If the sysop allows a user to post defamatory statements, for instance, the victim may sue for libel; if the operator deletes the posting, the author may sue for abridgment of free speech. Network operators, along with their attorneys and, ultimately, judges, will have to decide such issues case by case; the process of demarcating the boundaries of free speech online will therefore undoubtedly take years.

2. Laws and mores differ among towns, states, and countries. Whose rules apply in cyberspace?

Say that a New York City user downloads a favorite Sherlock Holmes story from a London computer. The works of Arthur Conan Doyle are in the public domain in the United Kingdom but some are still under copyright in the United States. Which country's law prevails? Or what happens if a member of the California bar offers to answer legal questions on a Usenet newsgroup. Is the attorney guilty of practicing law without a license outside California? Penthouse has created a World Wide Web edition whose first page instructs: "If you are accessing Penthouse Internet from any country or locale where adult material is specifically prohibited by law, go no further." Is that disclaimer enough? Or would Penthouse executives be wise to avoid any travel to a puritanical country where they might face prosecution? Such questions will pop up with increasing frequency as the Internet becomes more popular.

Because it spans the globe, the Net can subvert attempts by governments to restrict the flow of information. Ontario officials, for example, forbade publication of information about a particularly sensational murder case in an attempt to avoid an O.J. Simpson-like circus of publicity. The gag order did restrain mainstream media outlets but was swept away on the Internet when someone created a Usenet group called alt.fan.karla.homolka (the name of one of the defendants). After users began posting news and rumors concerning the case, officials ordered Canadian systems operators to delete the group from their storage disks. The operators complied--but some Canadians found they could easily use the Internet to reach the newsgroup from servers in the United States, Japan, or elsewhere.

The Homolka newsgroup isn't alone in evading national laws. According to reports in Ontario newspapers, the leader of a Canadian group that claims the Holocaust never happened plans to promote his views on the Net. The Canadian, Ernst Zundel, supposedly will use an Internet access provider based in the United States in hopes of avoiding prosecution under Canadian laws against hate mongering (on the Net, he'll find others of his ilk on the thriving newsgroup called alt.revisionism).

One need not even leave the United States to encounter a broad range of standards on acceptable forms of expression. Consider the saga of Robert and Carleen Thomas, a married couple in their late 30s living in California's Silicon Valley. Until four years ago, Robert had churned through a series of white-collar sales jobs on the fringes of the valley's booming, high-tech industries. Then he and Carleen found their own entrepreneurial niche. Working out of their tract home in Milpitas, they started the Amateur Action Bulletin Board System (AABBS), which enabled subscribers to download sexually explicit images and join in chat groups to discuss the materials.

The Thomases' digitized collection reached 20,000 images, largely gleaned from a photographer friend who once worked for Playboy and from magazines published abroad. The most frequently downloaded images depicted partially clad children, bestiality, and bondage. The Thomases promoted their service as "the nastiest place on earth," and advertised on the Net that they accepted Visa and MasterCard. By 1994, AABBS had more than 3,600 subscribers, each paying $99 per year for the privilege of accessing the collection.

Unhappily for the Thomases, they received too much publicity. In mid-1993, a Tennessee man surfing the Net came across an AABBS publicity post in the form of suggestive picture captions. The surfer, upset by what seemed to him to be child pornography, notified U.S. Postal Service authorities in Memphis. These officials activated Operation Longarm, a government anti-obscenity drive that focuses on child porn and, most recently, computer networks. As Longarm officials see it, the anonymous nature of the Internet makes it the perfect place for pedophiles to lurk.

The Memphis authorities assign-ed the complaint to postal investigator David Dirmeyer, who joined AABBS (under the alias "Lance White") and began downloading its images and tapping into its chat groups. Based on Dirmeyer's findings, postal investigators raided the Thomases' home in January 1994, armed with a 32-page search warrant, and seized computers, videotape-dubbing machines, and the AABBS database of photographs and videotapes. The couple was indicted, tried in federal district court in Memphis, and convicted of distributing obscene materials in interstate commerce. Last December, Robert Thomas was sentenced to 37 months; Carleen to 30 months.

The Thomas case reveals the difficulty of interpreting, in a world of computer networks, the meaning of "community standards"--the test by which a piece of work is to be judged obscene, according to the legal doctrine that the Supreme Court established in its 1973 decision in Miller v. California. In Miller, the Supreme Court ruled in effect that residents of Bible Belt towns need not put up with Times Square raunch. But in cyberspace, where physical proximity to an information source is unimportant, Miller- style community standards are essentially unenforceable.

Civil libertarians worry that if the Thomases' convictions hold, the Net will be governed by the standards of the most restrictive communities in the nation. In appealing their conviction, the Thomases argue that the materials they offered were not obscene by the standards of their Bay Area community. In fact, in 1992 the San Jose high-tech crime unit--essentially the Thomases' hometown police--seized the AABBS computers, scrutinized the collection of images, and found them insufficiently offensive to justify prosecution. In the United States, individuals have the constitutional right to own obscenity in the privacy of

their home, so long as the owner doesn't sell it, publicly display it, or show it to children; a Memphis citizen could therefore fly to San Francisco, purchase a book of AABBS-style photos, and bring it home without breaking any law. Many Net users and civil libertarians would like the courts to treat travel on the information superhighway in the same way--as if Lance White had motored to Milpitas. Indeed, some Thomas supporters argue that the international network of computers constitutes a "community" unto itself for Miller purposes, a frontier that cannot be subjected to offline restrictions. If the Net can't make its own law, then the natives at least want it insulated from the Memphises of the world.

But judges have rejected similar virtual-travel arguments concerning mail-order pornography and phone sex. In the 1989 phone sex case Sable Communications v. FCC, Sable argued that the government was creating "an impermissible national standard of obscenity" that forced providers "to tailor all their messages to the least tolerant community." The Supreme Court was unpersuaded, holding that "if Sable's audience is comprised of different communities with different local standards, Sable ultimately bears the burden of complying."

Courts are likely to treat online services the same way. An information provider may be expected to comply with the law's geographic limitations whenever access to its material is contingent on a transaction--such as the payment of money--that allows the purveyor to check the user's locale. Operators of computer bulletin board services, for example, would be made to ask for, and check on, users' locations. They may be required to use an 800 or 900 number that is programmed to block certain area codes, thus ensuring that people from conservative communities don't log on. The Thomases knew enough law to understand the hazards of letting underage users subscribe (they spot-checked names on credit card orders, calling the listed cardholder to be sure that he or she was the actual subscriber), but neither they nor their lawyer recognized the perils of community standards.

In this respect, members-only bulletin boards like the Thomases' hold less potential for charting new legal ground than cases where material is broadly available on the Internet. In fact, the Net offers many megabytes of raw and unsettling information, almost all of which can be obtained anonymously and for free; there is no way for a supplier of, say, pornographic pictures, to know whether those images are being downloaded in a Bible Belt town.

3. When offensive expression is distributed on a computer network, who is accountable?

Are people who post pornographic pictures to a Usenet newsgroup liable for obscenity in, say, Memphis, given that they had no way of knowing where images might be downloaded ? Would they be liable if children downloaded the images? For that matter, would the operators of an Internet access service in Memphis be liable for importing obscene material into town, or for making pornographic material (which adults can legally view) unlawfully accessible to children, merely for providing the conduit over which users reached such postings? The law is still murky on these questions of accountability.

As more and more people gain Net access through their schools and employers, such institutions are facing an uncertain future. At Santa Rosa Junior College in California, two female students were the subjects of sexually derogatory comments on a chat group restricted to male students. The women filed a civil rights claim against the college, arguing that the group violated federal law by excluding women and that the messages--discussing the two women in graphic "bathroom wall" language, according to one description--constituted sexual harassment. The students demanded that the journalism instructor who ran the online system be fired for aiding and abetting the harassment. The school hastily settled the suit, awarding the women cash compensation for both complaints and putting the instructor on indefinite administrative leave--and, in the process, exerting a considerable chilling effect on the people who run online services at other universities.

Academia isn't the only place where online sexual (or sexist) chatter will collide with freedom of speech. For example, if employers provide desktop access to Usenet discussion groups, including the gamy alt.sex hierarchy, could they be sued by women workers for creating a "hostile workplace?" In the past, courts have ruled that tacking up Playboy-style centerfolds on office bulletin boards can constitute sexual harassment of female workers--is the display of such images on computer screens any different?

The question of responsibility is also pivotal in a suit that Stratton Oakmont, a brokerage firm based in Lake Success, N.Y., brought against the Prodigy online service. Individuals sent a series of postings accusing Stratton Oakmont of criminal behavior and violations of Securities and Exchange Commission rules to Prodigy's "Money Talk" forum. Last year, Stratton Oakmont sued Prodigy for $200 million in libel damages. Prodigy lawyers argued that the service is a passive carrier of information, like the telephone company. Stratton Oakmont, however, countered that Prodigy is in the publishing business and is therefore responsible for all communication on its service.

A New York state judge ruled that Prodigy, which routinely screens postings for obscene or potentially libelous content, does in fact exert a form of editorial control over content on its system and could be sued as a publisher. Prodigy is appealing the state court's decision. (The man accused of writing the messages, a former Prodigy employee, says someone forged his ID. Such impersonation is relatively easy for even a journeyman hacker, and is bound to become more common--further muddying the waters of responsibility.)

In deciding whether Prodigy is liable for libelous material posted by its users, the appeals court will have to rely on few--and ambiguous--legal precedents. One court ruled that CompuServe was not responsible for material placed on its system by a subcontractor. Another court, however, held that a bulletin board operator was liable for copyright infringements perpetrated by its users. One certainty: if systems operators are deemed responsible, they will monitor users much more closely--and pass on the cost of new staff to their customers. User fees will increase as Net access providers spend money on legal fees fighting off lawsuits.

4. How can children be insulated from the Net's raunchier material?

A few years ago, protesters in Fresno, Calif., used a magnifying glass to find offensive textbook illustrations, including what they termed "phallic bicycle seats." A group in suburban New York City recently claimed that it had spotted a drawing of a topless bather in a beach scene in one of the Where's Waldo? children's books. After the threat of legal action, the book was removed from the school library shelves. It doesn't take a magnifying glass to find hard-core pornography on the Internet--and since many youngsters can navigate circles around their elders on the Net, some adults are in a near panic.

Not without reason. In one afternoon of online prospecting, we unearthed instructions for making bombs, an electronic pamphlet called "Suicide Methods," and a guide for growing marijuana at home. Besides NASA photos of Jupiter, worldwide weather reports, and the Library of Congress catalog, kids can access Penthouse, The Anarchist's Cookbook, and the poisonously anti-Semitic tract, Protocols of the Elders of Zion. It is as if every modem owner in the world--including porn fans, skinheads, bazooka lovers, anarchists, bigots, harassers, and Holocaust deniers--selects the books for everyone else's school library. As President Clinton told a meeting of the American Society of Newspaper Editors this spring, "It is folly to think that we should sit idly by when a child who is a computer whiz may be exposed to things on that computer which in some ways are more powerful, more raw, and more inappropriate than those from which we protect them when they walk in a 7-11."

Any user of the Internet can post pornography or sexual invitations to any unmoderated Usenet group: according to the Toronto arts paper Eye Weekly, a Canadian recently sent a

detailed post on oral sex to newsgroups populated by children. Moreover, the facelessness of the Net makes it impossible to determine who is accessing information. The manager of an adult bookstore can recognize and eject a 12- year-old; the operator of an Internet file archive cannot.

Several companies are now developing "lock-out" Internet accounts that block access to certain regions of the Net known to contain material inappropriate for children. Many online services, public schools, and universities block out particular Usenet groups-- often all of the alt.sex groups; sometimes only the most repugnant, such as alt.sex.pedophilia. Some sites have modified the Internet search tool Veronica to reject requests that include, for example, the word erotica. The American Library Association and other anticensorship organizations are keeping a watchful eye on these efforts to guard children--ready to oppose measures that tip the scales too far away from protection of free speech.

In any case, Net-savvy kids can breach such safeguards. If a school's Usenet system blocks the alt.sex groups, for example, a sufficiently motivated young hacker can use a common Internet tool called telnet to gain access to a system that does offer them. Such surfing gets even easier with the online menu system called gopher; the user can start at a "clean" site and, sooner or later, reach a "dirty" one. We started from the U.S. Department of Education's gopher server, for instance, and in seven gopher hops reached "The School Stopper's Textbook," which instructs students on how to blow up toilets, short-circuit electrical wiring, and "break into your school at night and burn it down." On the World Wide Web, with its tens of thousands of hyperlinks, similar short hops can whisk a student from a stuffy government site to an X-rated one. Even without access to gopher, telnet, or the Web, students can find plenty of inappropriate material; automated servers in Japan and elsewhere send out individual postings, including those from the alt.sex hierarchy, to anyone who sends the proper command through e-mail.

Most states have laws against giving children pornography, and some also prohibit providing minors with "dangerous information" (for example, guides to building explosives). Thus, in hopes of limiting their liability, many school districts are requiring parents to sign forms before their children can have Internet accounts--in effect, permission slips for virtual field trips. The lawyers drafting the documents are treading a fine line. A form vaguely referring to the possibility of "offensive material" may not hold up in court as proof that consent was adequately informed. On the other hand, a parental form that is too specific, spelling out the multifold possibilities of pornography, racism, sexism, munitions manuals, and all the rest, may frighten mom and dad into keeping the kids offline altogether--or into shopping for another school district.

Schools will do the best they can to corral children in safe cyberspaces. But will that be enough? Many onliners worry that Congress will in effect mandate that the entire Internet become a child-safe "Happynet." The political pressures may indeed prove irresistible, especially now that the Christian Coalition is lobbying for laws against online pornography. A Happynet Act would violate the First Amendment, but litigating the case up to the Supreme Court could take several years and hundreds of thousands of dollars.

5. How can creative artists protect their online work from digital theft?

A different kind of "free speech" issue involves the possible use of proprietary material. Writers have belatedly discovered that full texts of their copyrighted works are being marketed--without their permission and without compensation--by for-profit data- retrieval companies. Firms such as CARL Corp. and Information Access have in the past typed or electronically scanned in a published piece or writing, uploaded it to a database, and then charged customers for each online retrieval, or "hit."

Earlier this year, both the publishers of Modern Maturity magazine and the owners of the K-

Earlier this year, both the publishers of Modern Maturity magazine and the owners of the K-III group (which includes New York magazine, among others) ended agreements with Information Access; Reader's Digest has already severed its connections with CARL's UnCover service. In each case, executives not only wanted to retain potentially lucrative rights but were also responding to the threat of legal action from freelance writers for a share of online royalties.

In a similar conflict, litigation has gone beyond the threat stage. The National Writers Union (NWU), a spirited group representing freelance authors, has filed a federal suit against six large communications companies, including the New York Times, seeking damages for "electronic piracy." The suit alleges that the companies have been selling what they don't own, the electronic republication rights to freelancers' contributions-- rights that standard freelance contracts didn't cover. The case is slowly proceeding toward trial.

Writers' union representatives have been negotiating with several such services to work out an arrangement for assuring that electronic duplication of magazine articles and books will be accompanied by royalty payments. The precedent is the ASCAP system set up decades ago by the American Society of Composers, Authors, and Publishers, which provides that every time radio stations play a recording the creator gets a few pennies. As a result of these negotiations, some database services have promised to make reprint payments directly to authors who retain copyright.

One knotty issue is whether a "hit" on an electronic article more closely resembles republication in an anthology or sale of a back issue. This is an important distinction. Freelance writers ordinarily sell one-time publication rights for their magazine articles. If the magazine wants to reprint the article, in an anthology or elsewhere, it must pay the writer something extra. But if the magazine sells additional copies of a back issue, it doesn't owe the writer anything more.

To defend their territory, magazines and newspapers are redrafting their standard contracts to stipulate that writers are selling unlimited electronic rights along with one- time print rights. This development doesn't please writers' organizations, who worry that hungry freelancers will heedlessly sign away rights that may eventually prove valuable. In 1993, the National Writers Union urged the intellectual property working group of the Clinton administration's National Information Infrastructure initiative to prohibit publishers from contractually claiming "those rights (usually electronic-based rights) that do not yet exist, and/or those rights that, at the time of negotiation, lack a measurable economic value." Not surprisingly, publishers opposed the proposal; the administration, faced with more pressing business, did not push the issue. Established writers, meanwhile, have instructed their agents to shop new book projects around rather than sign over electronic rights--in some cases severing long-standing relationships with publishers as a result. Here, as elsewhere, the online technologies are reopening struggles that offline society thought it had settled decades ago.

Brave New Networks

These and other situations reflect the growing conflict between the law and computer-network technology. The legal mind constructs a time and computer-network space- bound world; cybernauts inhabit a world where physical location is immaterial. "Our laws didn't envision the Internet," says Larry Kramer, professor of constitutional law at New York University. In a notable effort to bridge the gap, a new Center for Informatics Law has been established at the John Marshall Law School in Chicago. The center promotes the need to create a separate set of principles just for cyberspace that may depart from the old common-law system.

Rhetorically, at least, the conflict between the old spatial laws and the new Net technology has been one-sided. The technologists are better poets, and they have appropriated the most

vibrant images to advance their cause. Indeed, the Progress and Freedom Foundation, a conservative Washington think tank, produced a document earlier this year with the less-than-modest title "Magna Carta for the Knowledge Age." The document talks grandly, if somewhat vaguely, of "liberation in cyberspace" from "rules, regulations, taxes and laws"--calling for, among other things, the abolition of the Federal Communications Commission.

In this way, the eager explorers of cyberspace like to draw a parallel between the emergence of the new world information order and the development of the frontier in the American West. This is the conceit promoted by the Electronic Frontier Foundation, which has been working since 1990 to promote online civil liberties. But we find two metaphorically opposed images of "the frontier." One is the heroic, colorized frontier of romantic fiction and television and movies, populated by manly sheriffs and spunky womenfolk. The other is the actual frontier, where life was often nasty, brutish, and short.

Eventually, in both fiction and fact, civilization arrived, bringing with it rules, social order, and taxes. To all but die-hard survivalists, this was regarded as progress. The Internet is now undergoing a similar transition, as the new, inchoate medium of unfettered individual freedom begins to evolve. The Wild West of the cyber-frontier is already morphing before our eyes--on the screen and in the courts.