Internet Law: Spring 2010
Professor Grimmelmann
New York Law School

Reading Packet 1

Introduction, Theory, and Jurisdiction

Contents

Class 1: Computers 3

Blown to Bits, ch. 1 3
Little Britain, Computer Says No 3
Kennison v. Daire 3
Pompeii Estates, Inc. v. Consolidated Edison Co. of N.Y., Inc. 4
NCIC Confidential Problem 7

Class 2: The Internet 9

Blown to Bits appendix 9
Internet Applications Checklist problem 9
Frank H. Easterbrook, Cyberspace and the Law of the Horse 10
Lawrence Lessig, The Law of the Horse: What Cyberlaw Might Teach 11

Class 3: "Cyberspace" 17

John Perry Barlow, A Declaration of the Independence of Cyberspace 17
Orin S. Kerr, The Problem of Perspective in Internet Law 19
David R. Johnson and David Post, Law and Borders 21
Voyeur Dorm Problem 25
Live-Shot Problem 26

Class 4: Law 28

Dow Jones & Co. v. Gutnick 29
Simson Garfinkel, Welcome to Sealand. Now Bugger Off 37

Class 5: Code 51

Jack Goldsmith and Timothy Wu, Digital Borders 52
James Fallows, The Connection Has Been Reset 58
Center for Democracy and Technology v. Pappert 64
Spam Problem 69

Class 6: Intermediaries 72

Marsh v. Alabama 73
Jeffrey Rosen, Google's Gatekeepers 75
Search King, Inc. v. Google Technologies., Inc. 83
Estavillo Problem 87
MAPS Problem 88

Class 7: Personal Jurisdiction 90

Young v. New Haven Advocate 91
Boschetto v. Hansing 96
TravelJungle Problem 101
Westside Story Problem 101
MSN Problem 102

CLASS 1: COMPUTERS

The first (and perhaps most important) of the four major course themes is whether and how law changes when computers—rather than people—make and enforce decisions. Thus, we begin our study of Internet Law with three cases in which the Internet doesn't even appear. These cases all involve people who've interacted with a computer in some form; the question facing a court should how to apply traditional legal standards once a computer enters the picture. I've deliberately chosen three areas of law—banking, public utilities, and civil rights—that aren't at all part of the rest of our curriculum. Don't worry about trying to learn the specific doctrines. Instead, determine what the rule would be if there weren't a computer involved, and then ask whether that rule makes sense in an "computerized" context. As we'll see—repeatedly—even when there's no doubt that law applies "to computers," figuring out *how* law applies in a new factual context can be a tricky problem.

Preparation Questions:

(1) "Can I have a word with the manager?" "Computer says no." What's the joke here? Have you had experiences like this? Why are computers so often associated with bureaucracy, frustration, and terrible customer service?

(2) The *Kennison* court implies that the result would have been different if the defendant had dealt with a human, rather than with a computer. Why? Would the result in *Pompeii Estates* have been different if the defendants there had dealt with a human, rather than a computer?

(3) Who programmed the computer in *Kennison*? Who programmed the computer in *Pompeii Estates*? How about the NCIC? Did any of them make design mistakes?

(4) Why did Easybank use a computer? Why did ConEd? How about the police arresting Buttle? What advantages does a computer provide? What are the disadvantages? Would society be better off if we prohibited the use of computers for these purposes altogether? If not, what safeguards do we need on their use?

(5) If you receive some information from a computer, are you allowed to take the computer at its word? If you put information into a computer, are you now responsible for all the consequences? What about the person who provides the computer? The person who programmed it? Who, if anyone, *ought* to be held responsible?

BLOWN TO BITS, ch. 1

Please read chapter 1 of *Blown to Bits*.

Little Britain, *Computer Says No*

Please watch the video at http://www.youtube.com/watch?v=7TYAQ0JWBzE.

Kennison v. Daire
High Court of Australia

[1986] HCA 4; (1986) 160 CLR 129

GIBBS C.J., MASON, WILSON, DEANE, DAWSON JJ.:

1. The appellant was convicted of larceny . . . . He was the holder of an Easybank card which enabled him to use the automatic teller machine of the Savings Bank of South Australia to withdraw money from his account with that bank. It was a condition of the use of the card that the customer's account could be drawn against to the extent of the funds available in that account. Before the date of the alleged offence, the appellant had closed his account and withdrawn the balance, but had not returned the card. On the occasion of the alleged offence, he used his card to withdraw $200 from the machine at the Adelaide branch of the bank. He was able to do so because the machine was off-line and was programmed to allow the withdrawal of up to $200 by any person who placed the card in the machine and gave the corresponding personal identification number. When off-line the machine was incapable of determining whether the card holder had any account which remained current, and if so, whether the account was in credit.

2. It is not in doubt that the appellant acted fraudulently with intent permanently to deprive the bank of $200. The appellant's submission is that the bank consented to the taking. It is submitted that the bank intended that the machine should operate within the terms of its programme, and that when it did so it gave effect to the intention of the bank.

3. In the course of an interesting argument, Mr Tilmouth pointed out that if a teller, having the general authority of the bank, pays out money on a cheque when the drawer's account is overdrawn, or on a forged order, the correct conclusion is that the bank intends that the property in the money should pass, and that the case is not one of larceny . . . . He submitted that, in effect, the machine was invested with a similar authority and that if, within the instructions in its programme, it handed over the money, it should be held that the property in the money passed to the card holder with the consent of the bank.

4. With all respect we find it impossible to accept these arguments. The fact that the bank programmed the machine in a way that facilitated the commission of a fraud by a person holding a card did not mean that the bank consented to the withdrawal of money by a person who had no account with the bank. It is not suggested that any person, having the authority of the bank to consent to the particular transaction, did so. The machine could not give the bank's consent in fact and there is no principle of law that requires it to be treated as though it were a person with authority to decide and consent. The proper inference to be drawn from the facts is that the bank consented to the withdrawal of up to $200 by a card holder who presented his card and supplied his personal identification number, only if the card holder had an account which was current. It would be quite unreal to infer that the bank consented to the withdrawal by a card holder whose account had been closed. The conditions of use of the card supplied by the bank to its customers support the conclusion that no such inference can be drawn. It is unnecessary to consider what the position might have been if the account had remained current but had insufficient funds to its credit. . . .

5. For these reasons . . . the appeal should be dismissed.

Pompeii Estates, Inc. v. Consolidated Edison Co. of N.Y., Inc.

Civil Court of the City of New York, Trial Term, Queens County
397 N.Y.S.2d 577 (1977)

Posner, J.:

The "Dawn of the Age of Aquarius" has also ushered in the "Age of the Computer".

There is no question that the modern computer is as indispensable to big business as the washing machine is to the American household. To ask the American housewife to go back to washing clothes by hand is as unthinkable as asking Consolidated Edison to send out its monthly bills by any other method than the computer.

This is an action in negligence by a builder against a public utility for damages sustained as a result of the alleged "wrongful" termination of electricity at an unoccupied one-family house (that had recently been constructed by the plaintiff) at 200-15 Pompeii Rd., Holliswood. Sometime in October, 1975, the defendant had installed electric services to the plaintiff's property. On or about January 20, 1976, the defendant terminated such service because of two unpaid bills amounting to $ 25.11. Since the premises were unoccupied, the lack of electricity caused the motor which operated the heating unit to go off, which resulted in frozen water pipes, which burst and caused $ 1,030 of proven damages to the premises. . . .

Defendant through the use of five witnesses, made out a good case proving that the notice to disconnect was probably mailed even though no witness had actual knowledge of mailing this specific notice. Obviously, it would be overly burdensome, if not impossible, to expect a utility mailing out thousands of disconnect notices a day to be able to prove that each one was individually mailed. . . .

Accordingly, this court finds that the defendant did comply with the statutory requirement of mailing even though we are also convinced that the plaintiff had never received the notice because an expert witness from the U. S. Postal Department testified that the postal service does not leave mail at an unoccupied address. Unless a statute or the contract between the parties calls for actual notice proof of mailing is sufficient to prove notice, even though the notice was never received.

While the parties, at the trial and in their memoranda of law devoted considerable time to the issue of "notice", the court finds that this is not the main issue in this case. Let us say that this was a "procedural" hurdle which Consolidated Edison cleared successfully. However, the court has serious doubts as to whether the defendant has cleared the "substantive" hurdle—did it act reasonably or negligently in discontinuing plaintiff's electric service?

. . . The defendant's witnesses stated that a customer's file is opened when a new account is established and that all correspondence and other documents involving the customer are included in this file. Defendant's attorney admitted that he had found in such file the original letter from plaintiff requesting the opening of electrical current. This letter is reproduced in its entirety because of its significance to the case:

> POMPEII ESTATES INC.
> 34-34 Bell Blvd.
> Bayside, N.Y. 11361
> 212-631-4466
>
> June 12, 1975

Con Edison
40-55 College Pt. Blvd.
Flushing, N.Y. 11354
Att: Mr. A. Vebeliunas—670-6152

To Whom It May Concern:

Please be advised that there have been no changes in the original Building Plans for the 2 Houses located at the following addresses:

House #1-200-15 Pompeii Rd., Holliswood, N.Y.—Lot #163

House #2—200-19 Pompeii Rd., Holliswood, N.Y.—Lot #160

Be further advised that the electrical load within the house will be:

6KW Lighting and 3 1/2 Horse Power Air-Conditioning

1/4 Horse Power Blowers

1.2 KW Dishwashers

There will be 1-150 AMP—3 wire socket type electric meter for each house.

Sincerely yours,
POMPEII ESTATES
AT: SWR
ALBINO TESTANI—PRESIDENT

Between the date of this letter (June 12, 1975) and the time service was installed (Oct. 24, 1975) four months elapsed. There was no other correspondence; but the plaintiff's witness (Testani) testified that he had numerous conversations with Mr. Vebeliunas on the phone and at the job site. Mr. Vebeliunas, defendant's employee never appeared in court, even though the case was tried on three separate occasions over a period of two weeks. Though Vebeliunas was defendant's field representative and the only contact plaintiff had with defendant, he was never consulted when the decision was made to discontinue service for the nonpayment of the first two months rent. The testimony of defendant's witnesses bore out the fact that said decision was a routine procedure activated by the computer and ordered by a Mr. Chris Hagan. Did defendant produce Mr. Hagan to testify what human input there was to the computer's order? No, like Mr. Vebeliunas, he never graced the courtroom scene. Failure to produce two key witnesses under the defendant's control can only lead to the inference that they would not contradict the plaintiff's contention that defendant acted unreasonably.

Negligence is lack of ordinary care. It is a failure to exercise that degree of care which a reasonably prudent person would have exercised under such circumstances. The statute only requires the notice of discontinuance to be sent to the premises where the service is provided; though, by regulation, the Public Service Commission has said that the customer may direct another address for mailing purposes. While the plaintiff's letter (supra) does not specifically direct that the mail be sent to 34-34 Bell Boulevard, any reasonably prudent person examining the letter would realize that this is a builder building new homes and that it is not customary for a builder to occupy the homes he builds. Certainly, any reasonably prudent person, if in doubt, would contact Mr. Vebeliunas to ascertain the facts. This is especially so when the termination of service is in the middle of winter and the foreseeable consequences to the heating system and the

water pipes are apparent. Where there is a foreseeability of damage to another that may occur from one's acts, there arises a duty to use care. In this instance, a one-minute cursory glance at plaintiff's letter (supra) would have alerted Mr. Hagan to the fact that there was something unusual in this situation. To the contrary, the computer said, "terminate," and Mr. Hagan gave the order to terminate.

This court finds the defendant liable to the plaintiff for damages in the amount of $ 1,030, with interest and costs. While the computer is a useful instrument, it cannot serve as a shield to relieve Consolidated Edison of its obligation to exercise reasonable care when terminating service. The statute gives it the discretionary power to do so, and this discretion must be exercised by a human brain. Computers can only issue mandatory instructions—they are not programmed to exercise discretion.

NCIC Confidential Problem

The following is a slightly edited version of the statement of facts in from *Rogan v. City of Los Angeles*, 668 F. Supp. 1384 (C.D. Cal. 1987):

> During 2006, Rollo Tomasi, an escapee from an Alabama state prison, started using Archibald Buttle's name after he obtained Buttle's birth certificate. Tomasi obtained the birth certificate at Saginaw, Michigan, Buttle's birthplace and place of residence.
>
> After obtaining Buttle's birth certificate, Tomasi proceeded to California. Tomasi there used Buttle's birth certificate to obtain a California driver's license and various other identification documents in Buttle's name.
>
> Sometime during 2007, Tomasi was arrested by the Los Angeles Police Department ("LAPD") on suspicion of murder. Tomasi was using the false identification in Buttle's name at the time of his arrest. The LAPD released Tomasi for reasons presently unknown.
>
> Approximately three months later, but still during 2007, Tomasi left Los Angeles and stopped using the identification in Buttle's name.
>
> On or about April 20, 2008, LAPD Lieutenant Dudley Smith caused an arrest warrant to issue in the name of Archibald Buttle, charging him with two robbery-murders that occurred in Los Angeles during April 2008. This warrant listed Buttle's name and an alias, but did not list Tomasi's known physical characteristics (e.g. Tomasi's scars and tattoos).
>
> On approximately May 10, 2008, another LAPD officer, Sergeant Ed Exley, caused the warrant information to be placed into the national computer arrest warrant notification system known as the National Crime Information Center ("NCIC"). Entry of this information into the NCIC system ensured that any police officer in the United States having access to the system would be made aware that a robbery-murder warrant in the name of Archibald Buttle was outstanding in California. Like the warrant upon which it was based, this information set forth Buttle's name and an alias, but did not contain Tomasi' known physical characteristics. . . .

On or about October 31, 2008, Buttle came into contact with Patrolman Jack Vincennes of the Carrollton Township Police Department in Saginaw County, Michigan, during the course of a trespassing dispute. Buttle was arrested a charge of disturbing the peace. Patrolman Vincennes made an inquiry of the NCIC system. The resulting computer report reflected the existence of the California robbery-murder warrant in Buttle's name.

On or about November 1, 2008, the Carrollton police contacted LAPD about the California arrest warrant. The Carrolton police established four days later through fingerprint comparison and Buttle's lack of certain scars and tattoos that were visible on the body of the wanted suspect, Tomasi, that Buttle was not the man wanted by the LAPD. Buttle then pleaded (either guilty or *nolo contendre*, the record does not reveal which) to the charge of resisting arrest and was sentenced to "time served" of five days, and released. Upon Buttle's initial arrest, the NCIC record regarding the California warrant was automatically removed from the NCIC system.

Later during November, 2008, LAPD Sergeant Exley caused the arrest warrant information in Buttle's name to be re-entered into the NCIC system without modifying same to reflect either the suspect's known unique physical characteristics (i.e. Tomasi's scars and tattoos) or the duplicate name/misidentification problem. As reflected by the relevant NCIC data entry form, a NCIC computer record contains a miscellaneous field that allows for the entry of up to 121 characters of information regarding identifying physical characteristics or possible duplicate name/mistaken identity situations.

During February or March, 2009, Buttle was a passenger in an automobile which was stopped by Bay County sheriff's deputy Bud White outside of Saginaw, Michigan, for failure to use a turn signal. Deputy White ran a computer check on Buttle after he showed his identification. The California robbery-murder warrant was reported back to White in response to the computer check. As a result, Buttle was ordered out of the car at gunpoint, searched, handcuffed, and transported to the jail in Bay City, Michigan. Buttle was there handcuffed to metal bars while Deputy White made telephone calls to the Saginaw police and the LAPD in order to determine Buttle's status. Buttle was released after being held in jail for approximately two hours.

Buttle has been arrested three more times, twice at gunpoint, by police in Michigan and Texas. Each time, he was released after his true identity was confirmed. He sought the assistance of the FBI, who confirmed that the NCIC contained a murder warrant in his name, but informed Buttle that "only the originating state agency (i.e. the LAPD) could delete, amend, or correct the computer warrant entry."

Buttle has come to you for legal advice. He would like to stop being arrested for crimes he didn't commit, and, if possible, recover damages for the past arrests. What, if anything, can he do? You may find it helpful to ask first whether he would have a remedy if it were the same police officer who arrested both Tomasi and Buttle, and then ask how the situation changes because two different police departments are involved, both of whom use the NCIC.

CLASS 2: THE INTERNET

Today, we bring the Internet into the picture. The bulk of the class will be lecture; I'll review the material from *Blown to Bits* and discuss how the Internet works on a technical level. But I've also given you some theoretical readings; these are two of the four most famous papers on Internet law. As we'll see, Lessig's "four modalities" offer a deeply useful way to think about online regulation. Easterbrook's paper, for its part, asks *the* fundamental question about Internet law: is there anything really different here, something not adequately covered in Torts, Contracts, etc.?

Preparation Questions:

(1) Judge Easterbook asks about cyberlaw, "Isn't this just the law of the horse?" What does he mean by "the law the of the horse?" Would you take a course in horse law? What are you hoping for from this course?

(2) Beneath Easterbrook's famous joke about *teaching* Internet law, there's a serious point about Internet law itself. He thinks it would be a mistake to create a specialized body of law to deal with it. Why not? Is it because he thinks the Internet doesn't represent any major changes, or because it's changing too fast? What does he recommend doing instead?

(3) Lessig talks about "four modalities of regulation." What are they? Give an example of each. Don't just repeat his examples. Think of your own. How are they different?

(4) In this course we'll talk a great deal about the Internet's "architecture." Is this the kind of architecture you can walk around in? Why does Lessig use that word to describe computer software? How can software substitute for law? How can software make law more effective? And how can software undermine legal control? The interrelationship between software and law is, of course, the first major theme of the course. But we'll see how it feeds into the others, as well.

Blown to Bits appendix

Please read the appendix of *Blown to Bits*.

Internet Applications Checklist problem

Here are some questions about common Internet applications that it's worth always keeping in mind.

(1) What can you do using this application?

(2) Does the application require that you and other users both be online at the same time? If so, how does the application figure out that you're both available?

(3) How does the message get from your computer to someone else's? Is it stored anywhere along the way? Who could listen in or read it if they wanted?

(4) How—in a very general sense—is the content encoded? Is it human-legible? Does its quality suffer in transit?

(5) Are there servers somewhere that assist in making the application available? If so, do they store the content, or do they merely assist in making connections? Could you make connections without the assistance of a server? Who's in charge of keeping those servers running, providing them with electricity, and so on?

(6) Do you need an account to post content? To receive it? How much information about yourself do you need to give up in order to take part?

(7) Who's allowed to post content, and of what sort? Is this an egalitarian medium, or one in which only a few people speak and the vast majority only listen?

(8) What happens "under the hood?" Is there a flow of information that you can describe in general terms, or does something so mysterious happen that it might as well be magic?

Do your best to answer these questions with respect to:

- The New York Times Online
- Jason Kottke's blog
- Email
- Amazon.com
- AIM (AOL Instant Messenger)
- Skype
- World of Warcraft
- Twitter
- Blackboard at NYLS
- YouTube
- Hulu
- Google
- Facebook

Frank H. Easterbrook, Cyberspace and the Law of the Horse
1996 U. CHI. LEGAL F. 207 (1996)

When he was dean of this law school, Gerhard Casper was proud that the University of Chicago did not offer a course in "The Law of the Horse." He did not mean by this that Illinois specializes in grain rather than livestock. His point, rather, was that "Law and . . ." courses should be limited to subjects that could illuminate the entire law. Instead of offering courses suited to dilettantes, the University of Chicago offered courses in Law and Economics, and Law and Literature, taught by people who could be appointed to the world's top economics and literature departments—even win the Nobel Prize in economics, as Ronald Coase has done.

I regret to report that no one at this Symposium is going to win a Nobel Prize any time soon for advances in computer science. We are at risk of multidisciplinary dilettantism, or, as one of my mentors called it, the cross-sterilization of ideas. Put together two fields about which you know little and get the worst of both worlds. Well, let me be modest. I am at risk of dilettantism, and I suspect that I am not alone. Beliefs lawyers hold about computers, and predictions they make about new technology, are highly likely to be false. This should make us hesitate to prescribe legal adaptations for cyberspace. The blind are not good trailblazers.

Dean Casper's remark had a second meaning—that the best way to learn the law applicable to specialized endeavors is to study general rules. Lots of cases deal with sales of horses; others deal with people kicked by horses; still more deal with the licensing and racing of horses, or with the care veterinarians give to horses, or with prizes at horse shows. Any effort to collect these strands into a course on "The Law of the Horse" is doomed to be shallow and to miss unifying principles. Teaching 100 percent of the cases on people kicked by horses will not convey the law of torts very well. Far better for most students—better, even, for those who plan to go into the horse trade—to take courses in property, torts, commercial transactions, and the like, adding to the diet of horse cases a smattering of transactions in cucumbers, cats, coal, and cribs. Only by putting the law of the horse in the context of broader rules about commercial endeavors could one really understand the law about horses.

Now you can see the meaning of my title. When asked to talk about "Property in Cyberspace," my immediate reaction was, "Isn't this just the law of the horse?" I don't know much about cyberspace; what I do know will be outdated in five years (if not five months!); and my predictions about the direction of change are worthless, making any effort to tailor the law to the subject futile. And if I did know something about computer networks, all I could do in discussing "Property in Cyberspace" would be to isolate the subject from the rest of the law of intellectual property, making the assessment weaker.

This leads directly to my principal conclusion: Develop a sound law of intellectual property, then apply it to computer networks. Problem: we do not know whether many features of existing law are optimal. Why seventeen years for patents, a lifetime plus some for copyrights, and forever for trademarks? Should these rights be strengthened or weakened? Why does copyright have the particular form it does? What sense can one make of the fuzzball factors for fair use? How can one make these rights more precise, and therefore facilitate Coasean bargains? Until we have answers to these questions, we cannot issue prescriptions for applications to computer networks. . . .

If we are so far behind in matching law to a well-understood technology such as photocopiers—if we have not even managed to create well-defined property rights so that people can adapt their own conduct to maximize total wealth—what chance do we have for a technology such as computers that is mutating faster than the virus in *The Andromeda Strain*? . . .

A quick summary: Error in legislation is common, and never more so than when the technology is galloping forward. Let us not struggle to match an imperfect legal system to an evolving world that we understand poorly. Let us instead do what is essential to permit the participants in this evolving world to make their own decisions. That means three things: make rules clear; create property rights where now there are none; and facilitate the formation of bargaining institutions. Then let the world of cyberspace evolve as it will, and enjoy the benefits.

Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*
113 Harv. L. Rev. 501 (1999)

A few years ago, at a conference on the "Law of Cyberspace" held at the University of Chicago, Judge Frank Easterbrook told the assembled listeners, a room packed with "cyberlaw" devotees (and worse), that there was no more a "law of cyberspace" than there was a "Law of the

Horse"; that the effort to speak as if there were such a law would just muddle rather than clarify; and that legal academics ("dilettantes") should just stand aside as judges and lawyers and technologists worked through the quotidian problems that this souped-up telephone would present. "Go home," in effect, was Judge Easterbrook's welcome.

As is often the case when my then-colleague speaks, the intervention, though brilliant, produced an awkward silence, some polite applause, and then quick passage to the next speaker. It was an interesting thought—that this conference was as significant as a conference on the law of the horse. (An anxious student sitting behind me whispered that he had never heard of the "law of the horse.") But it did not seem a very helpful thought, two hours into this day-long conference. So marked as unhelpful, it was quickly put away. Talk shifted in the balance of the day, and in the balance of the contributions, to the idea that either the law of the horse was significant after all, or the law of cyberspace was something more.

Some of us, however, could not leave the question behind. I am one of that some. I confess that I've spent too much time thinking about just what it is that a law of cyberspace could teach. This essay is an introduction to an answer.

. . . I agree that our aim should be courses that "illuminate the entire law," but unlike Easterbrook, I believe that there is an important general point that comes from thinking in particular about how law and cyberspace connect.

This general point is about the limits on law as a regulator and about the techniques for escaping those limits. This escape, both in real space and in cyberspace, comes from recognizing the collection of tools that a society has at hand for affecting constraints upon behavior. Law in its traditional sense—an order backed by a threat directed at primary behavior—is just one of these tools. The general point is that law can affect these other tools—that they constrain behavior themselves, and can function as tools of the law. The choice among tools obviously depends upon their efficacy. But importantly, the choice will also raise a question about values. By working through these examples of law interacting with cyberspace, we will throw into relief a set of general questions about law's regulation outside of cyberspace.

I do not argue that any specialized area of law would produce the same insight. I am not defending the law of the horse. My claim is specific to cyberspace. We see something when we think about the regulation of cyberspace that other areas would not show us.

[Example: Zoned Speech]

Porn in real space is zoned from kids. Whether because of laws (banning the sale of porn to minors), or norms (telling us to shun those who do sell porn to minors), or the market (porn costs money), it is hard in real space for kids to buy porn. In the main, not everywhere; hard, not impossible. But on balance the regulations of real space have an effect. That effect keeps kids from porn.

These real-space regulations depend upon certain features in the "design" of real space. It is hard in real space to hide that you are a kid. Age in real space is a self-authenticating fact. Sure—a kid may try to disguise that he is a kid; he may don a mustache or walk on stilts. But costumes are expensive, and not terribly effective. And it is hard to walk on stilts. Ordinarily a kid transmits that he is a kid; ordinarily, the seller of porn knows a kid is a kid, and so the seller of porn, either

because of laws or norms, can at least identify underage customers. Self-authentication makes zoning in real space easy.

In cyberspace, age is not similarly self-authenticating. Even if the same laws and norms did apply in cyberspace, and even if the constraints of the market were the same (as they are not), any effort to zone porn in cyberspace would face a very difficult problem. Age is extremely hard to certify. To a website accepting traffic, all requests are equal. There is no simple way for a website to distinguish adults from kids, and, likewise, no easy way for an adult to establish that he is an adult. This feature of the space makes zoning speech there costly - so costly, the Supreme Court concluded in *Reno v. ACLU*, that the Constitution may prohibit it.

[Cyberspace]

Many believe that cyberspace simply cannot be regulated. Behavior in cyberspace, this meme insists, is beyond government's reach. The anonymity and multi-jurisdictionality of cyberspace makes control by government in cyberspace impossible. The nature of the space makes behavior there unregulable.

This belief about cyberspace is wrong, but wrong in an interesting way. It assumes either that the nature of cyberspace is fixed—that its architecture, and the control it enables, cannot be changed—or that government cannot take steps to change this architecture.

Neither assumption is correct. Cyberspace has no nature; it has no particular architecture that cannot be changed. Its architecture is a function of its design—or, as I will describe it in the section that follows, its code. This code can change, either because it evolves in a different way, or because government or business pushes it to evolve in a particular way. And while particular versions of cyberspace do resist effective regulation, it does not follow that every version of cyberspace does so as well. Or alternatively, there are versions of cyberspace where behavior can be regulated, and the government can take steps to increase this regula[tion].

To see just how, we should think more broadly about the question of regulation. What does it mean to say that someone is "regulated"? How is that regulation achieved? What are its modalities?

[Modalities of Regulation]

Behavior, we might say, is regulated by four kinds of constraints. Law is just one of those constraints. Law (in at least one of its aspects) orders people to behave in certain ways; it threatens punishment if they do not obey. The law tells me not to buy certain drugs, not to sell cigarettes without a license, and not to trade across international borders without first filing a customs form. It promises strict punishments if these orders are not followed. In this way, we say that law regulates.

But not only law regulates in this sense. Social norms do as well. Norms control where I can smoke; they affect how I behave with members of the opposite sex; they limit what I may wear; they influence whether I will pay my taxes. Like law, norms regulate by threatening punishment ex post. But unlike law, the punishments of norms are not centralized. Norms are enforced (if at all) by a community, not by a government. In this way, norms constrain, and therefore regulate.

Markets, too, regulate. They regulate by price. The price of gasoline limits the amount one drives - more so in Europe than in the United States. The price of subway tickets affects the use of public transportation - more so in Europe than in the United States. Of course the market is

able to constrain in this manner only because of other constraints of law and social norms: property and contract law govern markets; markets operate within the domain permitted by social norms. But given these norms, and given this law, the market presents another set of constraints on individual and collective behavior.

And finally, there is a fourth feature of real space that regulates behavior—"architecture." By "architecture" I mean the physical world as we find it, even if "as we find it" is simply how it has already been made. That a highway divides two neighborhoods limits the extent to which the neighborhoods integrate. That a town has a square, easily accessible with a diversity of shops, increases the integration of residents in that town. That Paris has large boulevards limits the ability of revolutionaries to protest. That the Constitutional Court in Germany is in Karlsruhe, while the capital is in Berlin, limits the influence of one branch of government over the other. These constraints function in a way that shapes behavior. In this way, they too regulate.

These four modalities regulate together. The "net regulation" of any particular policy is the sum of the regulatory effects of the four modalities together. A policy trades off among these four regulatory tools. It selects its tool depending upon what works best.

So understood, this model describes the regulation of cyberspace as well. There, too, we can describe four modalities of constraint.

Law regulates behavior in cyberspace - copyright, defamation, and obscenity law all continue to threaten *ex post* sanctions for violations. How efficiently law regulates behavior in cyberspace is a separate question—in some cases it does so more efficiently, in others not. Better or not, law continues to threaten an expected return. Legislatures enact, prosecutors threaten, courts convict.

Norms regulate behavior in cyberspace as well: talk about democratic politics in the alt.knitting newsgroup, and you open yourself up to "flaming" (an angry, text-based response). "Spoof" another's identity in a "MUD" (a text-based virtual reality), and you may find yourself "toaded" (your character removed). Talk too much on a discussion list, and you are likely to wind up on a common "bozo" filter (blocking messages from you). In each case norms constrain behavior, and, as in real space, the threat of *ex post* (but decentralized) sanctions enforce these norms.

Markets regulate behavior in cyberspace too. Prices structures often constrain access, and if they do not, then busy signals do. (America Online (AOL) learned this lesson when it shifted from an hourly to a flat-rate pricing plan.) Some sites on the web charge for access, as on-line services like AOL have for some time. Advertisers reward popular sites; on-line services drop unpopular forums. These behaviors are all a function of market constraints and market opportunity, and they all reflect the regulatory role of the market.

And finally the architecture of cyberspace, or its code, regulates behavior in cyberspace. The code, or the software and hardware that make cyberspace the way it is, constitutes a set of constraints on how one can behave. The substance of these constraints varies—cyberspace is not one place. But what distinguishes the architectural constraints from other constraints is how they are experienced. As with the constraints of architecture in real space— railroad tracks that divide neighborhoods, bridges that block the access of buses, constitutional courts located miles from the seat of the government—they are experienced as conditions on one's access to areas of cyberspace. The conditions, however, are different. In some places, one must enter a password

before one gains access; in other places, one can enter whether identified or not. In some places, the transactions that one engages in produce traces, or "mouse droppings," that link the transactions back to the individual; in other places, this link is achieved only if the individual consents. In some places, one can elect to speak a language that only the recipient can understand (through encryption); in other places, encryption is not an option. Code sets these features; they are features selected by code writers; they constrain some behavior (for example, electronic eavesdropping) by making other behavior possible (encryption). They embed certain values, or they make the realization of certain values impossible. In this sense, these features of cyberspace also regulate, just as architecture in real space regulates.

These four constraints—both in real space and in cyberspace—operate together. For any given policy, their interaction may be cooperative, or competitive. Thus, to understand how a regulation might succeed, we must view these four modalities as acting on the same field, and understand how they interact.

[Choices Among Modalities]

Smoking and the Picture of Modern Regulation. Suppose the government seeks to reduce the consumption of cigarettes. There are a number of ways that the government could effectuate this single end. The law could, for example, ban smoking. (That would be law directly regulating the behavior it wants to change.) Or the law could tax cigarettes. (That would be the law regulating the supply of cigarettes in the market, to decrease their consumption.) Or the law could fund a public ad campaign against smoking. (That would be the law regulating social norms, as a means to regulating smoking behavior.) Or the law could regulate the nicotine in cigarettes, requiring manufacturers to reduce or eliminate the nicotine. (That would be the law regulating the "architecture" of cigarettes as a way to reduce their addictiveness and thereby to reduce the consumption of cigarettes.) Each of these actions can be expected to have some effect (call that its benefit) on the consumption of cigarettes; each action also has a cost. The question with each is whether the cost outweighs the benefit. If, for example, the cost of education to change norms about smoking were the same as the cost of changes in architecture, the value we place on autonomy and individual choice may tilt the balance in favor of education.

This is the picture of modern regulation. The regulator is always making a choice—a choice, given the direct regulations that these four modalities might effect, about whether to use the law directly or indirectly to some regulatory end. The point is not binary; the law does not pick one strategy over another. Instead, there is always a mix of direct and indirect strategies. The question the regulator must ask is: Which mix is optimal? . . .

[Conclusion]

At the center of any lesson about cyberspace is an understanding of the role of law. We must make a choice about life in cyberspace—about whether the values embedded there will be the values we want. The code of cyberspace constitutes those values; it can be made to constitute values that resonate with our tradition, just as it can be made to reflect values inconsistent with our tradition.

As the Net grows, as its regulatory power increases, as its power as a source of values becomes established, the values of real-space sovereigns will at first lose out. In many cases, no doubt, that is a very good thing. But there is no reason to believe that it will be a good thing generally or indefinitely. There is nothing to guarantee that the regime of values constituted by

code will be a liberal regime; and little reason to expect that an invisible hand of code writers will push it in that direction. Indeed, to the extent that code writers respond to the wishes of commerce, a power to control may well be the tilt that this code begins to take. Understanding this tilt will be a continuing project of the "law of cyberspace."

Nevertheless, Judge Easterbrook argued that there was no reason to teach the "law of cyberspace," any more than there was reason to teach the "law of the horse," because neither, he suggested, would "illuminate the entire law." This essay has been a respectful disagreement. The threats to values implicit in the law—threats raised by changes in the architecture of code—are just particular examples of a more general point: that more than law alone enables legal values, and law alone cannot guarantee them. If our objective is a world constituted by these values, then it is as much these other regulators—code, but also norms and the market—that must be addressed. Cyberspace makes plain not just how this interaction takes place, but also the urgency of understanding how to affect it.

CLASS 3: "CYBERSPACE"

Now that we have a tentative understanding of how the Internet works, we're ready to ask the same question we did about computers: what changes when we go online? We start with the most radical answer to that question, given by John Perry Barlow in 1996: "everything." He proposes that the Internet—or "cyberspace"—is a different place, naturally independent of earthbound governments, the same way that the American colonists argued that they were naturally independent of the British Crown in 1776. Orin Kerr, on the other hand, suggests that Barlow is trapped in the Matrix, beholden to an illusion created by computers.

Our two problems for today explore the idea that the Internet ought to be treated as its own jurisdiction. They both involve real-world governments trying to figure out whether the Internet is "here" or "there"—or perhaps both. As you answer them, try to figure out whether "here" versus "there" is even the right question to be asking.

Preparation Questions:

(1) What is Barlow's argument? This is one of the great manifestoes of all time, but try to figure out both what he's arguing against and what he's arguing for. What does this sort of "independence" mean? Freedom of thought and freedom of speech are central for him. Why are they so important—and so at risk—on the Internet?

(2) Johnson and Post's argument is different from Barlow's. How? What do they have in common with him? How would they respond to Judge Easterbrook's question about the law of the Internet being no different from traditional law?

(3) When you and I have a Skype videochat, what is happening in the internal perspective? How about from the external perspective?

(4) As you prepare the problems, try to ask how Barlow,, Kerr, and Post and Johnson would describe the two situations. Does this give you any insight into the laws at issue?

(5) Today's readings introduce our second major course theme: the effect of the Internet on governmental power. Take a first cut at it. Do you think the arrival of the Internet has increased or decreased the effective power of governments over individuals?

(6) The name of this course is "Internet Law" and in it, we've been talking about the "Internet." But the readings so far have used the terms "cyberlaw" and "cyberspace." Is there a difference between these terms? Does "cyberspace" exist?

John Perry Barlow, *A Declaration of the Independence of Cyberspace*
February 8, 1996

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You

have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.

Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions.

You have not engaged in our great and gathering conversation, nor did you create the wealth of our marketplaces. You do not know our culture, our ethics, or the unwritten codes that already provide our society more order than could be obtained by any of your impositions.

You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts. Many of these problems don't exist. Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different.

Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live.

We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth.

We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.

Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are based on matter. There is no matter here.

Our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion. We believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge. Our identities may be distributed across many of your jurisdictions. The only law that all our constituent cultures would generally recognize is the Golden Rule. We hope we will be able to build our particular solutions on that basis. But we cannot accept the solutions you are attempting to impose.

In the United States, you have today created a law, the Telecommunications Reform Act, which repudiates your own Constitution and insults the dreams of Jefferson, Washington, Mill, Madison, DeToqueville, and Brandeis. These dreams must now be born anew in us.

You are terrified of your own children, since they are natives in a world where you will always be immigrants. Because you fear them, you entrust your bureaucracies with the parental responsibilities you are too cowardly to confront yourselves. In our world, all the sentiments and expressions of humanity, from the debasing to the angelic, are parts of a seamless whole, the global conversation of bits. We cannot separate the air that chokes from the air upon which wings beat.

In China, Germany, France, Russia, Singapore, Italy and the United States, you are trying to ward off the virus of liberty by erecting guard posts at the frontiers of Cyberspace. These may

keep out the contagion for a small time, but they will not work in a world that will soon be blanketed in bit-bearing media.

Your increasingly obsolete information industries would perpetuate themselves by proposing laws, in America and elsewhere, that claim to own speech itself throughout the world. These laws would declare ideas to be another industrial product, no more noble than pig iron. In our world, whatever the human mind may create can be reproduced and distributed infinitely at no cost. The global conveyance of thought no longer requires your factories to accomplish.

These increasingly hostile and colonial measures place us in the same position as those previous lovers of freedom and self-determination who had to reject the authorities of distant, uninformed powers. We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies. We will spread ourselves across the Planet so that no one can arrest our thoughts.

We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before.

Davos, Switzerland

February 8, 1996

Orin S. Kerr, *The Problem of Perspective in Internet Law*
91 GEO. L. J. 357 (2003)

... In the 1999 science fiction thriller *The Matrix*, Keanu Reeves plays a computer hacker named "Neo" who learns that the reality he has known since birth is merely a virtual reality created by a computer network known as the Matrix. The *real* Neo lies in a semicomatose state attached to the network, to which he and others have been connected by advanced computers that have taken over the world and sap energy from humans while occupying their minds with virtual reality. Neo ends up joining the rebel forces trying to destroy the Matrix, and the movie jumps several times between the virtual world inside the Matrix and the real world outside of the Matrix. The movie presents us with two different realities, two existing worlds. The first reality is the virtual world that we experience inside the Matrix, and the second is the "real" world that we experience outside the Matrix.

In addition to being a fun movie, *The Matrix* points out an important problem that arises when we try to understand the nature of computer networks in general and the Internet in particular. Like Neo confronting the Matrix, we can think about the Internet in two ways, virtual and real. The virtual perspective is like the perspective inside the Matrix: it accepts the virtual world of cyberspace as akin to a reality. Of course, unlike Neo, we know all along that the virtual world that the computer generates is only virtual. But as we try to make sense of what the Internet is, to understand what we experience online, we might decide to treat that virtual world as if it were real.

I will call this virtual point of view the internal perspective of the Internet. The internal perspective adopts the point of view of a user who is logged on to the Internet and chooses to accept the virtual world of cyberspace as a legitimate construct. To this user, a computer connected to the Internet provides a window to a virtual world that is roughly analogous to the

physical world of real space. The user can use her keyboard and mouse to go shopping, send mail, visit a chat room, participate in an online community, or do anything else she can find online. The technical details of what the computers attached to the Internet actually do "behind the scenes" don't particularly matter. What matters is the virtual world of cyberspace that the user encounters and interacts with when he or she goes online.

We can also understand the Internet from a different perspective. Like Neo when he is outside the Matrix, we can look at the Internet from the point of view of the physical world, rather than the virtual one. I will call this the external perspective of the Internet. The external perspective adopts the viewpoint of an outsider concerned with the functioning of the network in the physical world rather than the perceptions of a user.

From this external viewpoint, the Internet is simply a network of computers located around the world and connected by wires and cables. The hardware sends, stores, and receives communications using a series of common protocols. Keyboards provide sources of input to the network, and monitors provide destinations for output. When the Internet runs properly, trillions of zeros and ones zip around the world, sending and receiving communications that the computers connected to the network can translate into commands, text, sound, and pictures.

From the external perspective, the fact that Internet users may perceive that they have entered a virtual world of cyberspace has no particular relevance. These perceptions reflect the fact that software designers often garnish their applications with icons, labels, and graphics to help novices understand and use them--for example, by writing e-mail programs so that e-mail looks and feels like postal mail. These superficialities have no deeper meaning from the external perspective. What matters is the physical network and the technical details of how it works, not the easily manipulated perceptions of Internet users.

Both internal and external understandings of the Internet should ring true to most of us. The Internet *is* a physical network, and it *can* create a virtual world for its users that can appear sufficiently realistic to its users to make a plausible claim for equal footing with the physical world. But the key for us is that by generating a virtual reality, the technology in a sense leaves us with two Internets, rather than one. We have an external version of the Internet, and also an internal one. One is physical, the other virtual. ...

Why does this matter to lawyers and to the nature of Internet law? It matters because legal outcomes depend on facts, and the facts of the Internet depend on which perspective we choose. This is a very practical problem. The basic task of a lawyer is to apply legal rules to facts—to apply law to an understanding of reality. In the case of the Internet, however, two competing understandings of reality exist. ...

All of this may seem rather abstract, so an example may help. Consider what happens when an Internet user surfs the web. Imagine that an Internet user opens up a web browser and types in "www.amazon.com," and moments later the homepage of Amazon.com appears on the viewer's screen. ...

This is easy from an internal perspective. The user has visited Amazon.com's website, going to Amazon.com's home on the Internet. The user has visited Amazon.com's virtual store much like a person might visit a store in the physical world, traveling from one point in cyberspace to another. ...

From an external perspective, however, the event appears quite different—and significantly more complicated. Behind the scenes, the simple act of typing "www.amazon.com" into a web browser triggers a series of responses from different computers connected to the Internet. The browser begins by sending out a request across the Internet to a special type of computer known as a Domain Name System (DNS) server. The browser's request asks the DNS server to translate the letters of the website address "amazon.com" into an "Internet Protocol" or "IP" address, which is a series of numbers that computers connected to the Internet understand as an address akin to a phone number. The DNS server will respond that "www.amazon.com" translates into the IP address "207.171.184.16." The user's browser then issues another request, this time directed to "207.171.184.16," asking it to send a set of data files back to the browser. Amazon.com's computer will receive the request and then send data back to the browser. The browser will receive the data and display it on the user's screen. The resulting images and text appear in the form of the Amazon. com webpage that the user requested.

Notice that the internal and external perspectives have produced two different accounts of the same event. One model of the facts follows the virtual perspective of the user, and another model follows the behind-the-scenes perspective of how the Internet actually works. From the internal perspective, visiting Amazon.com resembles visiting a store. The user types in the address, and a moment later is paying a virtual visit to Amazon.com's site. From the external perspective, visiting Amazon.com resembles calling Information and asking for Amazon.com's phone number, then dialing the number and asking the representative to send you the latest Amazon.com catalog. The single event of surfing the web produces two set of facts, one internal and the other external. As a result, when we need to apply law to the act of visiting a website, we can apply that law to two different sets of facts, which can produce two different outcomes.

David R. Johnson and David Post, *Law and Borders*
The Rise of Law in Cyberspace
48 STAN. L. REV. 1367 (1996)

I. Breaking Down Territorial Borders A. Territorial Borders in the "Real World"

We take for granted a world in which geographical borders — lines separating physical spaces — are of primary importance in determining legal rights and responsibilities. Territorial borders, generally speaking, delineate areas within which different sets of legal rules apply. There has until now been a general correspondence between borders drawn in physical space (between nation states or other political entities) and borders in "law space." For example, if we were to superimpose a "law map" (delineating areas where different rules apply to particular behaviors) onto a political map of the world, the two maps would overlap to a significant degree, with clusters of homogeneous applicable law and legal institutions fitting within existing physical borders. ...

2. When Geographic Boundaries for Law Make Sense.

Physical borders are not, of course, simply arbitrary creations. Although they may be based on historical accident, geographic borders for law make sense in the real world. Their logical relationship to the development and enforcement of legal rules is based on a number of related considerations.

Power. Control over physical space, and the people and things located in that space, is a defining attribute of sovereignty and statehood. Law-making requires some mechanism for law enforcement, which in turn depends on the ability to exercise physical control over, and impose coercive sanctions on, law-violators. For example, the U.S. government does not impose its trademark law on a Brazilian business operating in Brazil, at least in part because imposing sanctions on the Brazilian business would require assertion of physical control over business owners. Such an assertion of control would conflict with the Brazilian government's recognized monopoly on the use of force over its citizens.

Effects. The correspondence between physical boundaries and "law space" boundaries also reflects a deeply rooted relationship between physical proximity and the effects of any particular behavior. That is, Brazilian trade-mark law governs the use of marks in Brazil because that use has a more direct impact on persons and assets within Brazil than anywhere else. For example, a large sign over "Jones' Restaurant" in Rio de Janeiro is unlikely to have an impact on the operation of "Jones' Restaurant" in Oslo, Norway, for we may assume that there is no substantial overlap between the customers, or competitors, of these two entities. Protection of the former's trademark does not — and probably should not — affect the protection afforded the latter's.

Legitimacy. We generally accept the notion that the persons within a geographically defined border are the ultimate source of law-making authority for activities within that border. The "consent of the governed" implies that those subject to a set of laws must have a role in their formulation. By virtue of the preceding considerations, those people subject to a sovereign's laws, and most deeply affected by those laws, are the individuals who are located in particular physical spaces. Similarly, allocation of responsibility among levels of government proceeds on the assumption that, for many legal problems, physical proximity between the responsible authority and those most directly affected by the law will improve the quality of decision making, and that it is easier to determine the will of those individuals in physical proximity to one another.

Notice. Physical boundaries are also appropriate for the delineation of "law space" in the physical world because they can give notice that the rules change when the boundaries are crossed. Proper boundaries have signposts that provide warning that we will be required, after crossing, to abide by different rules, and physical boundaries — lines on the geographical map — are generally well-equipped to serve this signpost function.

B. The Absence of Territorial Borders in Cyberspace

... Cyberspace has no territorially based boundaries, because the cost and speed of message transmission on the Net is almost entirely independent of physical location. Messages can be transmitted from one physical location to any other location without degradation, decay, or substantial delay, and without any physical cues or barriers that might otherwise keep certain geographically remote places and people separate from one another. The Net enables transactions between people who do not know, and in many cases cannot know, each other's physical location. ...

[**Power**] But efforts to control the flow of electronic information across physical borders — to map local regulation and physical boundaries onto Cyberspace — are likely to prove futile, at least in countries that hope to participate in global commerce. Individual electrons can easily, and without any realistic prospect of detection, "enter" any sovereign's territory. The volume of electronic communications crossing territorial boundaries is just too great in relation to the resources available to government authorities. ...

By asserting a right to regulate whatever its citizens may access on the Net, these local authorities are laying the predicate for an argument that Singapore or Iraq or any other sovereign can regulate the activities of U.S. companies operating in Cyberspace from a location physically within the United States. All such Web-based activity, in this view, must be subject simultaneously to the laws of all territorial sovereigns.

[**Effects]** Nor are the effects of online activities tied to geographically proximate locations. Information available on the World Wide Web is available simultaneously to anyone with a connection to the global network. The notion that the effects of an activity taking place on that Web site radiate from a physical location over a geographic map in concentric circles of decreasing intensity, however sensible that may be in the nonvirtual world, is incoherent when applied to Cyberspace. A Web site physically located in Brazil, to continue with that example, has no more of an effect on individuals in Brazil than does a Web site physically located in Belgium or Belize that is accessible in Brazil. Usenet discussion groups, to take another example, consist of continuously changing collections of messages that are routed from one network to another, with no centralized location at all. They exist, in effect, everywhere, nowhere in particular, and only on the Net.

[**Legitimacy & Notice**] Territorial regulation of online activities serves neither the legitimacy nor the notice justifications. There is no geographically localized set of constituents with a stronger and more legitimate claim to regulate it than any other local group. The strongest claim to control comes from the participants themselves, and they could be anywhere. And in Cyberspace, physical borders no longer function as signposts informing individuals of the obligations assumed by entering into a new, legally significant, place. Individuals are unaware of the existence of those borders as they move through virtual space. ...

II. A New Boundary for Cyberspace

Traditional legal doctrine treats the Net as a mere transmission medium that facilitates the exchange of messages sent from one legally significant geographical location to another, each of which has its own applicable laws. But trying to tie the laws of any particular territorial sovereign to transactions on the Net, or even trying to analyze the legal consequences of Net-based commerce as if each transaction occurred geographically somewhere in particular, is most unsatisfying. A more legally significant, and satisfying, border for the "law space" of the Net consists of the screens and passwords that separate the tangible from the virtual world.

A. Cyberspace as a Place

Many of the jurisdictional and substantive quandaries raised by border-crossing electronic communications could be resolved by one simple principle: conceiving of Cyberspace as a distinct "place" for purposes of legal analysis by recognizing a legally significant border between Cyberspace and the "real world." Using this new approach, we would no longer ask

the unanswerable question "where" in the geographical world a Net-based transaction occurred. Instead, the more salient questions become: What procedures are best suited to the often unique characteristics of this new place and the expectations of those who are engaged in various activities there? What mechanisms exist or need to be developed to determine the content of those rules and the mechanisms by which they can enforced? Answers to these questions will permit the development of rules better suited to the new phenomena in question, more likely to be made by those who understand and participate in those phenomena, and more likely to be enforced by means that the new global communications media make available and effective.

1. The New Boundary is Real.

Treating Cyberspace as a separate "space" to which distinct laws apply should come naturally. There is a "placeness" to Cyberspace because the messages accessed there are persistent and accessible to many people. Furthermore, because entry into this world of stored online communications occurs through a screen and (usually) a password boundary, you know when you are "there." No one accidentally strays across the border into Cyberspace. To be sure, Cyberspace is not a homogenous place; groups and activities found at various online locations possess their own unique characteristics and distinctions, and each area will likely develop its own set of distinct rules. But the line that separates online transactions from our dealings in the real world is just as distinct as the physical boundaries between our territorial governments — perhaps more so. ...

B. Other Cyberspace Regimes

Once we take Cyberspace seriously as a distinct place for purposes of legal analysis, many opportunities to clarify and simplify the rules applicable to online transactions become available.

1. Defamation Law.

Treating messages on the Net as transmissions from one place to another has created a quandary for those concerned about liability for defamation: Messages may be transmitted between countries with very different laws, and liability may be imposed on the basis of "publication" in multiple jurisdictions with varying standards. In contrast, the approach that treats the global network as a separate place would consider any allegedly defamatory message to have been published only "on the Net" (or in some distinct subsidiary area thereof) — at least until such time as distribution on paper occurs. This re-characterization makes more sense. A person who uploads a potentially defamatory statement would be more able to determine the rules applicable to his own actions. Moreover, because the Net has distinct characteristics, including an enhanced ability of the allegedly defamed person to reply, the rules of defamation developed for the Net could take into account these technological capabilities -— perhaps by requiring that the opportunity for reply be taken advantage of in lieu of monetary compensation. The distinct characteristics of the Net could also be taken into account when applying and adapting the "public figure" doctrine in a context that is both global and highly compartmentalized and that blurs the distinction between private and public spaces. ...

III. Will Responsible Self-Regulatory Structures Emerge on the Net?

Even if we agree that new rules should apply to online phenomena, questions remain about who sets the rules and how they are enforced. We believe the Net can develop its own effective legal institutions. ...

IV. Local Authorities, Foreign Rules: Reconciling Conflicts

What should happen when conflicts arise between the local territorial law (applicable to persons or entities by virtue of their location in a particular area of physical space) and the law applicable to particular activities on the Net? The doctrine of "comity," as well as principles applied when delegating authority to self-regulatory organizations, provide us with guidance for reconciling such disputes.

The doctrine of comity, in the Supreme Court's classic formulation, is "the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens or of other persons who are under the protections of its law." ... Comity arose as an attempt to mitigate some of the harsher features of a world in which lawmaking is an attribute of control over physical space but in which persons, things, and actions may move across physical boundaries. It functions as a constraint on the strict application of territorial principles that attempts to reconcile "the principle of absolute territorial sovereignty [with] the fact that intercourse between nations often demands the recognition of one sovereign's lawmaking acts in the forum of another." In general, comity reflects the view that those who care more deeply about and better understand the disputed activity should determine the outcome. Accordingly, it may be ideally suited to handle, by extension, the new conflicts between the nonterritorial nature of cyberspace activities and the legitimate needs of territorial sovereigns and of those whose interests they protect on the other side of the cyberspace border. This doctrine does not prevent territorial sovereigns from protecting the interests of those individuals located within their spheres of control, but it calls upon them to exercise a significant degree of restraint when doing so. ...

Because controlling the flow of electrons across physical boundaries is so difficult, a local jurisdiction that seeks to prevent its citizens from accessing specific materials must either outlaw all access to the Net — thereby cutting itself off from the new global trade — or seek to impose its will on the Net as a whole. This would be the modern equivalent of a local lord in medieval times either trying to prevent the silk trade from passing through his boundaries (to the dismay of local customers and merchants) or purporting to assert jurisdiction over the entire known world. ...

Voyeur Dorm Problem

This problem is based on *Voyeur Dorm L.C. v. City of Tampa*, 121 F. Supp. 2d 1373 (2000), *rev'd* 265 F.3d 1232 (2001).

Voyeur Dorm is a limited-liability company that operates a web site at voyeurdorm.com. The web site features 24-hour live video feeds from a house at 2312 West Farwell Drive, in a residential neighborhood of Tampa, Florida. Those videos show the lives of the residents of 2312 West Farwell, five women who who are under contracts with Voyeur Dorm specifying that they are employed to appear on a "'stage and filming location,' with 'no reasonable expectation of privacy,' for 'entertainment purposes.'" The nature of those purposes can be gleaned from

the descriptions on the voyeurdorm.com website, which states, "The girls of Voyeur Dorm are fresh, naturally erotic and as young as 18. Catch them in the most intimate acts of youthful indiscretion." Subscribers pay $34.95 a month for access to the web site. The address of the house is not listed on the web site, and the activities inside the house are not visible from outside.

The City of Tampa brings an action against Voyeur Dorm to enforce its zoning code, which prohibits "adult entertainment" uses in residential areas (including the area where house is located). The zoning code defines "adult entertainment," in relevant part, as:

> "Any premises . . . on which is offered to members of the public or any person, for a consideration, entertainment featuring or in any way including specified sexual activities, as defined in this section, or entertainment featuring the displaying or depicting of specified anatomical areas, as defined in this section; 'entertainment' as used in this definition shall include, but not be limited to, books, magazines, films, newspapers, photographs, paintings, drawings, sketches or other publications or graphic media, filmed or live plays, dances or other performances distinguished by their display or depiction of specified anatomical areas or specified anatomical activities, as defined in this section."

Voyeur Dorm defends on the basis that the house at 2312 West Farwell Drive is not a "premises . . . on which [adult entertainment] is offered to members of the public."

(1) Is Voyeur Dorm in violation of the Tampa zoning ordnance?

(2) Would it make a different to your analysis to learn the location of Voyeur Dorm's corporate offices? The servers from which voyeurdorm.com operates? Voyeurdorm.com's subscribers?

Live-Shot Problem

Sylvia Moreno, *Mouse Click Brings Home Thrill of the Hunt*, WASH. POST, May 8, 2005:

> On a tranquil Central Texas landscape, three fallow deer wandered through live oak and cedar as a rifle barrel poked out of a small shack nearby. With a metallic click, the Remington, clutched in a motorized steel cradle without a hunter at the trigger, swiveled to track them.
>
> The gun's scope showed the cross hairs settle right behind a buck's shoulder and hold steady, a perfect aim that would kill the animal in one clean shot — if the hunter wanted to fire the gun. More than 1,300 miles away in Indiana, looking at his computer screen, he decided to pass. This hunter wants to bag a blackbuck antelope, and he will wait to click the computer mouse that will send the electronic signal to shoot.
>
> It is called hunting by remote control, the brainchild of Texas entrepreneur John Lockwood, whose Internet business advertises a "real time on-line hunting and shooting experience."
>
> The business, Live-Shot, is open to everyone who registers and pays monthly $14.95 membership dues and a $1,000 deposit toward the cost of the animal. People using the service must have a valid Texas hunting license, which can be obtained online.

> The Remington .30-06 rifle is mounted atop a homemade contraption of welded metal and a piece of butcher block, and is attached to a small motor, three video cameras (two linked to the Internet, including the one embedded in the gun scope) and a door lock actuator, like that used in a car. The actuator is attached to a wire that pulls the trigger at the click of the mouse. From virtually anywhere, someone with an Internet connection can fire the rifle.
>
> If most hunters use blinds to conceal themselves from deer or other wildlife, "what is the difference in this and clicking a mouse?" asked Lockwood as he pulled the trigger of an unloaded Winchester Model 70 .30-06 that he uses for hunting. "Nothing. That is the same exact motion, and it takes the same amount of time."

(1) The Texas Parks and Wildlife Department allows live, in-person deer hunting but has promulgated a regulation stating, "A person may not engage in computer-assisted remote hunting of any animal or bird or provide or operate facilities for computer-assisted remote hunting if the animal or bird being hunted is located in Texas." Under this regulation, may Texas punish the operators of live-shot.com? Live-shot.com's users in Illinois? Is the regulation a good idea, in light of the readings for today?

(2) Illinois has enacted a statute providing, "A person shall not operate, provide, sell, use, or offer to operate, provide, sell, or use any computer software or service that allows a person not physically present at the hunt site to remotely control a weapon that could be used to take wildlife by remote operation, including, but not limited to, weapons or devices set up to fire through the use of the Internet or through a remote control device." Under this statute, may Illinois punish the operators of live-shot.com in Texas? Live-shot.com's users in Illinois? Is the statute a good idea, in light of the readings for today?

(3) Does it matter that a state agency promulgated the regulation in (1) whereas the state legislature enacted the statute in (2)? Should it matter?

CLASS 4: LAW

Barlow's natural-law argument that cyberspace is *somewhere else* hasn't fared well. But the argument that it's either a *bad idea* or *too hard* for offline governments to regulate the Internet has done better. Today we take up in earnest the question of whether offline governments should exercise control over what happens online. The key juxtaposition is between Johnson and Post—who would generally say "no"—and the *Gutnick* case—whose answer is an emphatic "yes." The third major reading, the article about Sealand and HavenCo, discusses an attempt to make the question moot by showing that governments *can't* effectively control the Internet because it flows over national borders.

Taken together, today's readings raise a disturbing possibility: that the Internet forces us to choose between total anarchy or total national control online. Either anything goes and all national values except the most libertarian are toast, or nothing goes and the most restrictive rule anywhere in the world controls the Internet everywhere. Is that really the choice, and if it is, which way is it likely to go?

Preparation Questions

(1) One way of looking at *Gutick* is as a response to Johnson and Post. Why might Australia be unwilling to treat the Internet as lying beyond its borders? What interests does it have that are threatened by the Internet? How would Johnson and Post respond?

(2) Another way of looking at *Gutnick* is as a conflict, not between Australia and the Internet, but between the U.S. and Australia. Reread Judge Callinan's discussion of the alleged defamation. This case probably couldn't have been brought in a United States court. Why not? If the court dismisses the case, has the U..S effectively imposed its free-speech values on Australia? If the court allows it to proceed, has Australia effectively imposed its values on the United States? This tension isn't new, but why does the existence of the Internet exacerbate it?

(3) A user posted a mobile-phone video of Italian schoolchildren taunting an autistic classmate to YouTube. Google took the video down, but not quickly enough in the view of prosecutors. They arrested Peter Fleischer, the company's chief privacy officer., when he was in Milan to give a speech at a conference; he now faces a potential one-year prison sentence, as do three other Google executives, including its chief legal officer. For more on the case, see Eric Pfanner, *Google Faces a Different World in Italy*, N.Y. TIMES (Dec. 13, 2009). In light of today's readings, any thoughts?

(4) Alternatively, consider the running dispute between the U.S. and most of the rest of the world over online poker. Although betting on horse races over the Internetis generally permitted in the U.S. and some states permit Internet lotteries, the federal government has cracked down increasingly hard on Internet poker sites. The issue came to a head after the U.S. arrested and prosecuted the operators of Internet poker sites based in the island nation of Antigua, including one Jay Cohen. This resulted in a World Trade Organization complaint claiming that U.S. restrictions on Internet poker violate the U.S.' treaty obligations to allow competition in "recreational, cultural and sporting services." For more on the story, see Paul Blustein, *Against All Odds*, WASH. POST (Aug. 4, 2006). This raises three questions. First, why did Cohen and his colleagues set up shop in Antigua, rather than in the U.S.?

Second, why didn't going offshore work for them? And third, will the WTO be able to do a good job resolving this sort of conflict? Finally, do you have any better ideas?

(5) With all that in mind, let's think about Sealand. What is a "data haven," and why did locating itself on abandoned World War II gunnery platform allow HavenCo to offer one? Why would the Jay Cohens of the world want to use one? How does the existence of Sealand affect our conversations about governmental control of the Internet? Is it checkmate for national values?

(6) But there's a twist: HavenCo failed. Even its domain is dead. What went wrong? Why might it have failed? Did HavenCo make dumb mistakes, or was the whole plan inherently doomed from the start? What could HavenCo offer its users, and was that was a good deal from their perspective? What could what governments (or disgruntled private actors) do if HavenCo's clients started causing them a lot of trouble? What makes governments legitimate and stable, and is HavenCo able to say the same?

(7) Finally, back to a big theme. Does the Internet increase or decrease governmental power? Has your answer changed since last time?

Dow Jones & Co. v. Gutnick
High Court of Australia
[2002] HCA 56

GLEESON CJ, McHUGH, GUMMOW AND HAYNE JJ. The appellant, Dow Jones & Company Inc ("Dow Jones"), prints and publishes the Wall Street Journal newspaper and Barron's magazine. Since 1996, Dow Jones has operated WSJ.com, a subscription news site on the World Wide Web. Those who pay an annual fee (set, at the times relevant to these proceedings, at $US59, or $US29 if they are subscribers to the printed editions of either the Wall Street Journal or Barron's) may have access to the information to be found at WSJ.com. Those who have not paid a subscription may also have access if they register, giving a user name and a password. The information at WSJ.com includes Barron's Online in which the text and pictures published in the current printed edition of Barron's magazine are reproduced.

The edition of Barron's Online for 28 October 2000 (and the equivalent edition of the magazine which bore the date 30 October 2000) contained an article entitled "Unholy Gains" in which several references were made to the respondent, Mr Joseph Gutnick. Mr Gutnick contends that part of the article defamed him. He has brought an action in the Supreme Court of Victoria against Dow Jones claiming damages for defamation. Mr Gutnick lives in Victoria. He has his business headquarters there. Although he conducts business outside Australia, including in the United States of America, and has made significant contributions to charities in the United States and Israel, much of his social and business life could be said to be focused in Victoria.

The originating process in the action which Mr Gutnick brought against Dow Jones was served on it outside Australia. ...

Undisputed principles

Argument of the appeal proceeded from an acceptance, by both parties, of certain principles. First, it is now established that an Australian court will decline, on the ground of *forum*

non conveniens, to exercise jurisdiction which has been regularly invoked by a plaintiff, whether by personal service or under relevant long-arm jurisdiction provisions, only when it is shown that the forum whose jurisdiction is invoked by the plaintiff is clearly inappropriate. Secondly, it is now established that in trying an action for tort in which the parties or the events have some connection with a jurisdiction outside Australia, the choice of law rule to be applied is that matters of substance are governed by the law of the place of commission of the tort. Neither party sought to challenge either proposition. Rather, argument focused upon where was the place of publication of the statements of which Mr Gutnick complained. Dow Jones contended that the statements were published in New Jersey and that it was, therefore, the law of that jurisdiction which would govern all questions of substance in the proceeding. ...

Dow Jones has its editorial offices for Barron's, Barron's Online and WSJ.com in the city of New York. Material for publication in Barron's or Barron's Online, once prepared by its author, is transferred to a computer located in the editorial offices in New York city. From there it is transferred either directly to computers at Dow Jones's premises at South Brunswick, New Jersey, or via an intermediate site operated by Dow Jones at Harborside, New Jersey. It is then loaded onto six servers maintained by Dow Jones at its South Brunswick premises. ...

The principal burden of the argument advanced by Dow Jones on the hearing of the appeal in this Court was that articles published on Barron's Online were published in South Brunswick, New Jersey, when they became available on the servers which it maintained at that place.

In the courts below, much weight appears to have been placed by Dow Jones on the contention that a relevant distinction was to be drawn between the apparently passive role played by a person placing material on a web server from which the would-be reader had actively to seek the material by use of a web browser and the (comparatively) active role played by a publisher of a widely circulated newspaper or a widely disseminated radio or television broadcast. In this Court, these arguments, though not abandoned, were given less prominence than policy arguments based on what was said to be the desirability of there being but a single law governing the conduct of a person who chooses to make material available on the World Wide Web.

Dow Jones submitted that it was preferable that the publisher of material on the World Wide Web be able to govern its conduct according only to the law of the place where it maintained its web servers, unless that place was merely adventitious or opportunistic. Those who, by leave, intervened in support of Dow Jones generally supported this contention. The alternative, so the argument went, was that a publisher would be bound to take account of the law of every country on earth, for there were no boundaries which a publisher could effectively draw to prevent anyone, anywhere, downloading the information it put on its web server. ...

It is necessary to begin by making the obvious point that the law of defamation seeks to strike a balance between, on the one hand, society's interest in freedom of speech and the free exchange of information and ideas (whether or not that information and those ideas find favour with any particular part of society) and, on the other hand, an individual's interest in maintaining his or her reputation in society free from unwarranted slur or damage. The way in which those interests are balanced differs from society to society. In some cases, for example as between the States in Australia, the differences in substantive law might be said to be differences of detail rather than substance, although even then it may be doubted that this is an accurate characterisation of the effect of the differences in the defamation laws of the Australian States.

Whether or not that is so, comparing the law of defamation in different countries can reveal differences going well beyond matters of detail lying at the edge of debate. ...

The tort of defamation, at least as understood in Australia, focuses upon publications causing damage to reputation. It is a tort of strict liability, in the sense that a defendant may be liable even though no injury to reputation was intended and the defendant acted with reasonable care. Yet a publication made in the ordinary course of a business such as that of bookseller or news vendor, which the defendant shows to have been made in circumstances where the defendant did not know or suspect and, using reasonable diligence, would not have known or suspected was defamatory, will be held not to amount to publication of a libel. There is, nonetheless, obvious force in pointing to the need for the publisher to be able to identify, in advance, by what law of defamation the publication may be judged. But it is a tort concerned with damage to reputation and it is that damage which founds the cause of action. ...

Harm to reputation is done when a defamatory publication is comprehended by the reader, the listener, or the observer. Until then, no harm is done by it. This being so it would be wrong to treat publication as if it were a unilateral act on the part of the publisher alone. It is not. It is a bilateral act — in which the publisher makes it available and a third party has it available for his or her comprehension. ...

In the course of argument much emphasis was given to the fact that the advent of the World Wide Web is a considerable technological advance. So it is. But the problem of widely disseminated communications is much older than the Internet and the World Wide Web. The law has had to grapple with such cases ever since newspapers and magazines came to be distributed to large numbers of people over wide geographic areas. Radio and television presented the same kind of problem as was presented by widespread dissemination of printed material, although international transmission of material was made easier by the advent of electronic means of communication.

It was suggested that the World Wide Web was different from radio and television because the radio or television broadcaster could decide how far the signal was to be broadcast. It must be recognised, however, that satellite broadcasting now permits very wide dissemination of radio and television and it may, therefore, be doubted that it is right to say that the World Wide Web has a uniquely broad reach. It is no more or less ubiquitous than some television services. In the end, pointing to the breadth or depth of reach of particular forms of communication may tend to obscure one basic fact. However broad may be the reach of any particular means of communication, those who make information accessible by a particular method do so knowing of the reach that their information may have. In particular, those who post information on the World Wide Web do so knowing that the information they make available is available to all and sundry without any geographic restriction.

Because publication is an act or event to which there are at least two parties, the publisher and a person to whom material is published, publication to numerous persons may have as many territorial connections as there are those to whom particular words are published. It is only if one starts from a premise that the publication of particular words is necessarily a singular event which is to be located by reference only to the conduct of the publisher that it would be right to attach no significance to the territorial connections provided by the several places in which the publication is available for comprehension. ...

In defamation, the same considerations that require rejection of locating the tort by reference only to the publisher's conduct, lead to the conclusion that, ordinarily, defamation is to be located at the place where the damage to reputation occurs. Ordinarily that will be where the material which is alleged to be defamatory is available in comprehensible form assuming, of course, that the person defamed has in that place a reputation which is thereby damaged. It is only when the material is in comprehensible form that the damage to reputation is done and it is damage to reputation which is the principal focus of defamation, not any quality of the defendant's conduct. In the case of material on the World Wide Web, it is not available in comprehensible form until downloaded on to the computer of a person who has used a web browser to pull the material from the web server. It is where that person downloads the material that the damage to reputation may be done. Ordinarily then, that will be the place where the tort of defamation is committed. ...

Three other matters should be mentioned. In considering what further development of the common law defences to defamation may be thought desirable, due weight must be given to the fact that a claim for damage to reputation will warrant an award of substantial damages only if the plaintiff has a reputation in the place where the publication is made. Further, plaintiffs are unlikely to sue for defamation published outside the forum unless a judgment obtained in the action would be of real value to the plaintiff. The value that a judgment would have may be much affected by whether it can be enforced in a place where the defendant has assets

Finally, if the two considerations just mentioned are not thought to limit the scale of the problem confronting those who would make information available on the World Wide Web, the spectre which Dow Jones sought to conjure up in the present appeal, of a publisher forced to consider every article it publishes on the World Wide Web against the defamation laws of every country from Afghanistan to Zimbabwe is seen to be unreal when it is recalled that in all except the most unusual of cases, identifying the person about whom material is to be published will readily identify the defamation law to which that person may resort.

The appeal should be dismissed with costs.

KIRBY J.

... The nature of the Web makes it impossible to ensure with complete effectiveness the isolation of any geographic area on the Earth's surface from access to a particular website. Visitors to a website automatically reveal their Internet Provider ("IP") address. This is a numerical code that identifies every computer that logs onto the Internet. The visitor may also disclose certain information about the type of browser and computer that the visitor uses. The IP addresses of users are generally assigned to them by an Internet Service Provider ("ISP"). The user's IP address will remain the same whenever and wherever the user "surfs" the Web. But some ISPs do not assign a permanent IP address. Instead, they assign a new IP address every time a user logs onto the Web. Because of these features, there is presently no effective way for a website operator to determine, in every case, the geographic origin of the Internet user seeking access to the website.

For similar reasons, with respect to subscription accounts, checking the issuing location of a credit card provided by a user would not afford a universally reliable means of ascertaining the geographic location of a user seeking access to a website. Thus, even assuming that a geographic restriction could be introduced isolating Australia (and hence Victoria) by reference to the origin

of the visitor's credit card, a resident of Australia with a credit card issued by a United States bank, would be able to access sites that might be denied to an Australian resident with an Australian credit card, although both users were physically located in Australia.

In addition to these difficulties of controlling access to a website by reference to geographic, national and subnational boundaries, the Internet has recently witnessed a rapid growth of technologies ("anonymising technologies") that enable Internet users to mask their identities (and locations). By reason of these developments, the provision of cost effective, practical and reliable identity verification systems, that could afford a universally reliable recognition of the point of origin of an Internet user, has not emerged. This is why the nature of Internet technology itself makes it virtually impossible, or prohibitively difficult, cumbersome and costly, to prevent the content of a given website from being accessed in specific legal jurisdictions when an Internet user in such jurisdictions seeks to do so. In effect, once information is posted on the Internet, it is usually accessible to all Internet users everywhere in the world. Even if the correct jurisdiction of an Internet user could be ascertained accurately, there is presently no adequate technology that would enable non-subscription content providers to isolate and exclude all access to all users in specified jurisdictions.

These special features of the Internet present peculiar difficulties for the legal regulation of its content and, specifically, for the exclusion of access in defined jurisdictions. Such difficulties may have a bearing on the question of whether a particular jurisdiction has an advantage in regulating content published and accessed on the Internet. This does not mean (and no party before the Court suggested) that the Internet is, or should be, a law-free zone. However, in considering what the law, and specifically the common law of Australia, should say in relation to the contents of the Internet, particularly with respect to allegedly defamatory material on a website, the appellant argued that regard had to be taken of these elementary practical features of the technology. ...

The law in different jurisdictions, reflecting local legal and cultural norms, commonly strikes different balances between rights to information and expression and the protection of individual reputation, honour and privacy. These disparities suggest the need for a clear and single rule to govern the conduct in question according to pre-established norms. If it is to be effective, such a rule must be readily ascertainable. To tell a person uploading potentially defamatory material onto a website that such conduct will render that person potentially liable to proceedings in courts of every legal jurisdiction where the subject enjoys a reputation, may have undesirable consequences. Depending on the publisher and the place of its assets, it might freeze publication or censor it or try to restrict access to it in certain countries so as to comply with the most restrictive defamation laws that could apply. Or it could result in the adoption of locational stratagems in an attempt to avoid liability.

A new rule for a unique technology: In response to the suggestion that similar questions have existed at least since telegraph and international shortwave radio and that such potential liability is a commonplace in the world of global television distributed by satellite, the appellant pointed to the peculiarities of Internet publication. Viewed in one way, the Internet is not simply an extension of past communications technology. It is a new means of creating continuous relationships in a manner that could not previously have been contemplated. According to this view, the Internet is too flexible a structure to be controlled by a myriad of national laws, purportedly applied with no more justification than is provided by the content of such laws,

usually devised long before the Internet arrived. For stored information, accessible in cyberspace, the new technology was said to demand a new approach. This would be true as much for the law of taxation, commercial transactions and other areas, as for the law of defamation. ...

Whilst the Internet does indeed present many novel technological features, it also shares many characteristics with earlier technologies that have rapidly expanded the speed and quantity of information distribution throughout the world. I refer to newspapers distributed (and sometimes printed) internationally; syndicated telegraph and wire reports of news and opinion; newsreels and film distributed internationally; newspaper articles and photographs reproduced instantaneously by international telefacsimile; radio, including shortwave radio; syndicated television programmes; motion pictures; videos and digitalised images; television transmission; and cable television and satellite broadcasting. Generally speaking, it is undesirable to express a rule of the common law in terms of a particular technology. Doing so presents problems where that technology is itself overtaken by fresh developments. It can scarcely be supposed that the full potential of the Internet has yet been realised. The next phase in the global distribution of information cannot be predicted. A legal rule expressed in terms of the Internet might very soon be out of date. ...

In a cause of action framed in defamation, the publication of the material which damages the reputation of the plaintiff is essential. Merely creating and making the material available is insufficient. The material has to be accessed or communicated in a jurisdiction where the plaintiff has a reputation. That will usually be the place where the plaintiff is resident. Unlike product liability or some other negligence claims, damage to reputation cannot occur "fortuitously" in a place outside of the defendant's contemplation. Where a person or corporation publishes material which is potentially defamatory to another, to ask the publisher to be cognisant of the defamation laws of the place where the person resides and has a reputation is not to impose on the publisher an excessive burden. At least it is not to do so where the potential damage to reputation is substantial and the risks of being sued are commensurately real. Publishers in the United States are well aware that few, if any, other jurisdictions in the world observe the approach to the vindication of reputation adopted by the law in that country.

The foregoing approach may pose problems, particularly in cases where the plaintiff has a substantial reputation in more than one legal jurisdiction and seeks to recover for the damage in all such jurisdictions in a single proceeding. In such a case, potential liability in defamation for the publication of material relating to such a person on the Internet may indeed have a chilling effect on free speech merely because one of those jurisdictions has more restrictive defamation laws than the others. This approach could subject Australian defendants to the more restrictive defamation laws of foreign jurisdictions. However, such problems are the result of the absence of uniformity in defamation laws, combined with an ability to access and broadcast material across national boundaries (which is not limited to the Internet) and the absence of international treaties or reciprocal laws to govern those issues. Problems of a similar nature will arise whatever test is adopted for choice of law purposes unless this Court were to revert to a parochial approach of answering all questions in proceedings properly founded in an Australian forum by reference only to the law of that forum. ...

Conclusion: The present case does not present an acute example of the foregoing difficulties. To the knowledge of the appellant, the respondent ordinarily resided in Victoria. He had his business address there. He was an officer there of several companies listed on the

Australian Stock Exchange. He was prominent in the local Jewish (Lubavitcher) community. He was also well known there for charitable and sporting interests.

True, some readers of Barron's Online, or Barron's magazine with access to the appellant's website in New Jersey (or in New York), would have known of the respondent. Arguably, an action based on the tort of defamation could therefore also be brought in those jurisdictions of the United States. However, in this case it could not be suggested that the respondent had resorted to Victoria only in order to invoke the process of its courts or in an exercise of forum shopping. So far as damage to his reputation was concerned, Victoria, as the place of his residence, was where most such damage would be done, rather than amongst business, religious or other acquaintances in North America or with the very large number of strangers there who might read about the respondent in the appellant's Internet publications. ...

The dismissal of the appeal does not represent a wholly satisfactory outcome. Intuition suggests that the remarkable features of the Internet (which is still changing and expanding) makes it more than simply another medium of human communication. It is indeed a revolutionary leap in the distribution of information, including about the reputation of individuals. It is a medium that overwhelmingly benefits humanity, advancing as it does the human right of access to information and to free expression. But the human right to protection by law for the reputation and honour of individuals must also be defended to the extent that the law provides.

The notion that those who publish defamatory material on the Internet are answerable before the courts of any nation where the damage to reputation has occurred, such as in the jurisdiction where the complaining party resides, presents difficulties: technological, legal and practical. It is true that the law of Australia provides protections against some of those difficulties which, in appropriate cases, will obviate or diminish the inconvenience of distant liability. Moreover, the spectre of "global" liability should not be exaggerated. Apart from anything else, the costs and practicalities of bringing proceedings against a foreign publisher will usually be a sufficient impediment to discourage even the most intrepid of litigants. Further, in many cases of this kind, where the publisher is said to have no presence or assets in the jurisdiction, it may choose simply to ignore the proceedings. It may save its contest to the courts of its own jurisdiction until an attempt is later made to enforce there the judgment obtained in the foreign trial. It may do this especially if that judgment was secured by the application of laws, the enforcement of which would be regarded as unconstitutional or otherwise offensive to a different legal culture.

However, such results are still less than wholly satisfactory. They appear to warrant national legislative attention and to require international discussion in a forum as global as the Internet itself. ...

CALLINAN J.

The question which this case raises is whether the development of the Internet calls for a radical shift in the law of defamation. ...

It is unnecessary to set out the whole of the article. The first three paragraphs sketch some of the interests of the respondent. The fourth states that some of his business dealings with religious charities raise "uncomfortable questions". The author then uses some language that the media have appropriated from the law courts, implying that a balanced trial with equal

opportunity to participate by all concerned has taken place: that a "Barron's investigation found that several charities traded heavily in stocks promoted by Gutnick." (emphasis added) The article associates the respondent with Mr Nachum Goldberg who is apparently a convicted tax evader and another person awaiting trial for stock manipulation in New York.

A detailed discussion of various of the respondent's religious and political activities and business dealings follows. One paragraph of the article claims that an intercepted communication from the convicted tax evader was taken by Australian prosecutors to mean that the respondent was the former's "biggest money-laundering customer". ...

The respondent brought proceedings against the appellant in defamation in the Supreme Court of Victoria. After an amendment of his statement of claim he alleged publication both online and by hard copies sold in Australia. He pleaded that the article meant, and was understood to mean that he:

> was a customer of Nachum Goldberg who had recently been imprisoned for tax evasion and money laundering; and
>
> was Nachum Goldberg's biggest customer; and
>
> was masquerading as a reputable citizen when he was, in fact, a tax evader who had laundered large amounts of money through Nachum Goldberg; and
>
> had bought Nachum Goldberg's silence so as to conceal his identity as one of Goldberg's customers."

... A publisher, particularly one carrying on the business of publishing, does not act to put matter on the Internet in order for it to reach a small target. It is its ubiquity which is one of the main attractions to users of it. And any person who gains access to the Internet does so by taking an initiative to gain access to it in a manner analogous to the purchase or other acquisition of a newspaper, in order to read it.

The appellant contends that the Internet is not "pushed" into any particular jurisdiction. The contention ignores the commercial and social realities that greater publication produces both greater profit and broader persuasion. Indeed, the appellant's arguments would suggest that all of its objectives were exclusively high-minded. Revenues from increased advertising and circulation, and the word "profit" never passed the appellant's advocate's lips. It may well be that "firewalls" to deny access to the unintended or non-subscribing reader are at present perhaps imperfect. So be it. Publishers are not obliged to publish on the Internet. If the potential reach is uncontrollable then the greater the need to exercise care in publication. ...

I disagree. The most important event so far as defamation is concerned is the infliction of the damage, and that occurs at the place (or the places) where the defamation is comprehended. Statements made on the Internet are neither more nor less "localized" than statements made in any other media or by other processes. Newspapers have always been circulated in many places. The reach of radio and television is limited only by the capacity of the technology to transmit and hear or view them, which already, and for many years, has extended beyond any one country. In any event, a "publisher", whether on the Internet or otherwise, will be likely to sustain only nominal, or no damages at all for publication of defamatory matter in a jurisdiction in which a person defamed neither lives, has any interests, nor in which he or she has no reputation to

vindicate. Furthermore, it may be that an action inadvisably brought in such a jurisdiction might be met by a finding that the jurisdiction is not a convenient or appropriate forum.

The appellant argued that the respondent, having set out to make money in the United States, must expect to be subjected to lawful scrutiny in that country. No doubt the fact of lawful scrutiny in that country, if such the publication was, would provide a defence to the appellant to defamation proceedings there. That fact does not however have anything to say about unlawful publication in this country.

The Court was much pressed with arguments about the ubiquity of the Internet. That ubiquity, it was said, distinguished the Internet from practically any other form of human endeavour. Implicit in the appellant's assertions was more than a suggestion that any attempt to control, regulate, or even inhibit its operation, no matter the irresponsibility or malevolence of a user, would be futile, and that therefore no jurisdiction should trouble to try to do so. I would reject these claims. Some brands of motor cars are ubiquitous but their manufacturers, if they wish to sell them in different jurisdictions must comply with the laws and standards of those jurisdictions. There is nothing unique about multinational business, and it is in that that this appellant chooses to be engaged. If people wish to do business in, or indeed travel to, or live in, or utilise the infrastructure of different countries, they can hardly expect to be absolved from compliance with the laws of those countries. The fact that publication might occur everywhere does not mean that it occurs nowhere. Multiple publication in different jurisdictions is certainly no novelty in a federation such as Australia.

The appellant invited the Court to prefer, in effect, a United States jurisdiction to an Australian one because the latter would deprive it of the Constitutional protection available in the former. ...

Australian defamation law, and, for that matter, English defamation law also, and the policy underlying them are different from those of the United States. There is no doubt that the latter leans heavily, some might say far too heavily, in favour of defendants. Nor has the metaphor for free speech developed by Holmes J in a series of cases and beginning with his dissenting judgment in *Abrams v United States*, a marketplace of ideas, escaped criticism in the United States. ...

Quite deliberately, and in my opinion rightly so, Australian law places real value on reputation, and views with scepticism claims that it unduly inhibits freedom of discourse. In my opinion the law with respect to privilege in this country, now and historically, provides an appropriate balance which does justice to both a publisher and the subject of a publication. ...

I agree with the respondent's submission that what the appellant seeks to do, is to impose upon Australian residents for the purposes of this and many other cases, an American legal hegemony in relation to Internet publications.

Simson Garfinkel, *Welcome to Sealand. Now Bugger Off*
WIRED (July 2000)

Ryan Lackey, a 21-year-old MIT dropout and self-taught crypto expert, sees fantastic things for himself in 2005. For starters, he'll be filthy rich. But his future is animated by more than just

money — to wit, the exploration of a huge idea he thinks will change the world. Lackey's big concept? That freedom is the next killer app.

Before you get too choked up, you should know that Lackey means giving corporations and frisky individuals the "freedom" to store and move data without answering to anybody, including competitors, regulators, and lawyers. He's part of a crew of adventurers and cypherpunks that's working to transform a 60-year-old gunnery fort in the North Sea — an odd, quasi-independent outpost whose British owner calls it "the Principality of Sealand" — into something that could be possible only in the 21st century: a fat-pipe Internet server farm and global networking hub that combines the spicier elements of a Caribbean tax shelter, Cryptonomicon, and 007.

This summer, with $1 million in seed money provided by a small core of Internet-fattened investors, Lackey and his colleagues are setting up Sealand as the world's first truly offshore, almost-anything-goes electronic data haven — a place that occupies a tantalizing gray zone between what's legal and what's ... possible. Especially if you exist, as the Sealanders plan to, outside the jurisdiction of the world's nation-states. Simply put: Sealand won't just be offshore. It will be off-government.

The startup is called, fittingly, HavenCo Ltd. Headquartered on a 6,000-square-foot, World War II-era antiaircraft deck that comprises the "land" of Sealand, the facility isn't much to look at and probably never will be. It consists of a rusty steel deck sitting on two hollow, chubby concrete cylinders that rise 60 feet above the churn of the North Sea. Up top there's a drab

building and a jury-rigged helicopter landing pad.

Soon, Lackey believes, powerful upgrades will transform Sealand into something amazing. The huge support cylinders will contain millions of dollars' worth of networking gear: computers, servers, transaction processors, data-storage devices — all cooled with banks of

roaring air conditioners and powered by triple-redundant generators. HavenCo will provide its clients with nearly a gigabit per second of Internet bandwidth by year's end, at prices far cheaper than those on the overregulated dry land of Europe — whose financial capitals sit a mere 20 milliseconds away from Sealand's electronic nerve center. Three speedy connections to HavenCo affiliate hubs all over the planet — microwave, satellite, and underwater fiber-optic links — will ensure that the data never stops flowing.

HavenCo's onboard staff will come and go on helicopters and speedboats. Four security people will be on hand at all times to maintain order; six computer geeks will run the network operations center. The security personnel, heavily armed and ready to blast anybody who shouldn't be around, will make sure that unauthorized boats and aircraft keep their distance. The geeks will perform maintenance tasks like replacing failed hard disks and installing new equipment. These routine chores will be a little more challenging than usual, given the maritime setting and Sealand's obsession with privacy. Fall over the edge of Sealand's deck, for instance, and you'll probably drown. Simply entering one of the machine rooms will require putting on scuba gear, because the rooms will be filled with an unbreathable pure nitrogen atmosphere instead of the normal oxygen mix — a measure designed to keep out sneaks, inhibit rust, and reduce the risk of fire.

HavenCo will be "offshore" both physically and in the sense that its clients — who will purchase preconfigured "colocation" computers maintained and secured by HavenCo — will basically be able to tell the rest of the world to shove it. The essence of offshore Internet services, as defined by sort-of-offshore places like Anguilla and Bermuda, is that when you base an operation in such a locale, you can claim to be governed only by the laws that prevail there. So if Internet gambling is legal (or overlooked) in Country A but not in Country B, you set up in A, and use the Web to send your site to B — and to the rest of the world.

Similarly, companies using Sealand to house their data can choose to operate according to the special laws of Sealand, and those laws will be particularly lax — though not quite anarchic. Lackey says the general idea is to allow a little naughtiness, while forbidding criminal activity that could generate international outrage.

Meaning? Basically, that HavenCo wants to give people a safe, secure shelter from lawyers, government snoops, and assorted busybodies without getting tangled in flagrant wrongdoing. So if you run a financial institution that's looking to operate an anonymous and untraceable payment system — HavenCo can help. If you'd like to send old-fashioned, adults-only pornography into a grumpy country like Saudi Arabia — HavenCo can help there, too. But if you want to run a spamming operation, launder drug money, or send kiddie porn anywhere — forget it.

To visualize a typical HavenCo customer circa 2005, imagine a company we'll call MacroMaxx, a Berlin-based construction giant that has offices throughout the world. MacroMaxx wants a secure new data center for its European offices, so the firm clicks on to the www.havenco.com Web site and purchases access to a Sealand-based server hooked up to an IBM RAID machine, which gives it a terabyte of online storage. The system is already installed and running in HavenCo's machine room. After putting through a confirmed bank transfer, MacroMaxx instantly gets the computer's password. Its technicians configure the standard set of server applications, then start building user accounts. Within an hour, email is moving.

The server's location on Sealand means MacroMaxx won't have to worry about fires, earthquakes, tornadoes, thefts, bomb threats, industrial sabotage, or killer-bee attacks. Or, for that matter, the discovery process in civil suits. If MacroMaxx is embroiled in a legal tussle and doesn't feel cooperative, it could use Sealand's unique status as a way to dig in its heels. Say, for example, that a pesky court official shows up at the company's Berlin office with a disk-duplicating device, demanding all company email for the past year. MacroMaxx execs could say, "Gee, we don't have that here." The official would be stymied, because the email simply wouldn't be on the premises, and it's up to MacroMaxx whether it keeps any backups around. The primary data would be housed only at Sealand.

And should the authorities find out and call Sealand demanding to come aboard and access MacroMaxx's machines? No problem, says Lackey: They'll be told to bugger off.

That's the vision, anyway. The current reality is more mundane. Sealand does exist — it's a real, live, passport-issuing, artificial micronation that's been around since 1967, arguably the only remotely credible place like it in the world. But there's a lot of work left to be done, as I saw firsthand on a dim and stormy day in March.

HavenCo will allow online gambling, pyramid schemes, and adult pornography — but spamming and corporate cybersabotage are out.

Sealand was originally called Roughs Tower; it was built as part of a complex of no-frills antiaircraft forts designed for shooting down Nazi planes on bombing runs to England. The old battle station stands in 24 feet of North Sea brine, 6 miles east of Felixstowe, an industrial port on the southeast coast of England. Abandoned after the war, the structure was occupied in '67 by Roy Bates, a British war veteran who renamed it Sealand, declared its independence from Great Britain, and appointed himself its "prince."

He got away with it, too — sort of. Officially, the UK doesn't recognize Sealand, but except for a few dustups now and then, the government has left the strange little fief alone.

The bigger challenge for Bates has been figuring out what to do with it. Over the years, Roy (the royal patriarch, now 78), his wife, Joan (also known as Princess Joan, 70), and his son, Michael (the dauphin-style heir apparent, 47), have earned their livings through fairly ordinary pursuits — like commercial fishing and fish processing — while shuttling back and forth between the platform and the mainland and styling themselves dual citizens of Sealand and the UK. They've theorized about various moneymaking plans — pirate radio outposts, tax havens, pleasure dens, casinos — but in the end, Sealand has been a money pit. The Bateses say they've spent huge amounts on upkeep, supplies, legal fees, and improvements.

When Sealand does blip on the geopolitical radar, it usually involves a brand of low comedy that has made it a favorite of Fleet Street journalists. In 1997, for example, an Andrew Cunanan/Sealand connection surfaced. After Gianni Versace's killer committed suicide on a Miami houseboat, police discovered that the man who owned the boat was in possession of a purported Sealand passport. Nothing more came of it, but as it turns out, lots of people have Sealand passports who shouldn't — the things apparently self-replicate without the Bateses' knowledge. This past spring, Sealand made the news again: Law-enforcement officials in Spain busted a Madrid-based gang allegedly tied to international drug trafficking and money laundering. The gang appeared to be using a fake Sealand Web site and thousands of phony Sealand passports as part of its criminal activity.

Questioned by Interpol, Roy wailed about the injustice of anyone using the Sealand name for black deeds. "[Sealand] has all been a game, an adventure, and it is very unfortunate to see it take this turn," he told one reporter.

"Nobody is more honest than my husband," Joan said at the time. "He's so honest he creaks."

Whether or not HavenCo counts as creakingly honest, it isn't the sort of enterprise you'd expect to come from a 78-year-old fisherman, and it didn't. In this deal, Roy is a cheerful cosignatory, but it was Michael who forged the pact with the cypherpunks. Michael is also the only "royal family" member on board when I go along for the weekly resupply mission to Sealand, which shoves off from the town of Southend-on-Sea — where Michael and a partner run a shellfish-processing factory — at 4:30 am sharp.

Our boat, the *Paula Maree*, pulls away from the coast toting enough canned food and drinking water to feed Sealand's current two-man crew for another week. Today the vessel is carrying more interesting stuff, including steel girders, a winch, an electric arc welder, an oxyacetylene torch, and a welding tank. The construction materials are for use in building a new crane that will hoist aboard still more building supplies, generators, power conditioners, batteries, and fuel tanks. If all goes according to plan, Sealand will support millions of dollars worth of networking equipment and computer racks by late summer.

It takes 15 minutes to get to Sealand by helicopter, but our trip will take five hours because we're starting 45 miles southwest of the site. The *Paula Maree*'s captain, a clean-shaven, compact fisherman named Mason West, guides the vessel using a combination of navigational beacons and GPS. Ryan Lackey and Michael Bates are on board, along with two burly security guards, Alan Beale and Bill Alen, who will spend the next week doubling as construction workers.

The cockpit is jammed, so Bates sends Lackey and me down below. Lackey is short and pudgy, with the requisite shaved head of a new media hipster. He's obviously intelligent, and seems driven to do something major before he's 25. After scoring 1,580 on his SATs, he skipped his last year of high school and entered MIT in 1996. But he quit after three years for lack of tuition money — he now describes himself as a "crypto-hacker/crypto-anarchist who happened to be attending MIT" — and went to work as a programmer for a highly secretive electronic payments startup that he cofounded, then abandoned, on the Caribbean island of Anguilla. After his failed stint there, he moved to San Francisco, his home base during the busy period leading up to the HavenCo launch.

Michael Bates comes down the ladder. He and Lackey start talking about pending renovations to Sealand's electrical system. Lackey, thinking big, wants to buy three large generators, a couple of industrial-size power conditioners, and a hefty bank of batteries to run the computers in an emergency. "I'd like to shoot for five minutes of battery backup," he says, explaining that if two of the running generators simultaneously fail, five minutes should be enough time to get the third operational. "We'll use gel cells."

"How many thousand pounds?" Bates asks. He means the weight, not the price: HavenCo's existing crane can barely lift 800 pounds.

Lackey shrugs: dunno. He shrugs again when I recommend conventional lead-acid batteries, because gel cells have a limited shelf life. "Five years from now," he says, hitting me with a serious gaze, "we are either going to be completely broke or we're going to be fantastically wealthy."

Sounds far-fetched, but who knows? HavenCo has collected its key employees, studied the relevant (and confusing) international law, and scooped up the money needed to get going. Along with Lackey, major personnel include Sean Hastings and his wife, Jo, who have experience in programming, offshore financing, and online gambling. Another important player is Sameer Parekh, a computer security specialist who launched the crypto software company C2Net and is now HavenCo's chair. Parekh confidently predicts HavenCo will pull in between $50 million and $100 million in profits by the end of its third year in business.

That remains to be seen — Lackey says he has plenty of clients lined up, but for "security reasons," he can name only one of them: Tibet Online, the Net presence of Tibet's exiled government, which is eager to escape the clutches of the Chinese government. Lackey also intimates an impending partnership with a major corporation he expects will resell HavenCo colocation space to customers with the highest security demands. Before HavenCo had even signed any clients, the project attracted decent investment money from serious people. Two Internet millionaires have publicly jumped aboard: Avi Freedman, Akamai's 30-year-old VP of network architecture, is investing $500,000; and Joichi Ito, the 34-year-old chair of Infoseek Japan, is kicking in $200,000. (A group of anonymous backers has also ponied up $400,000.) That's not a lot as startups go, but HavenCo doesn't need much to get off the ground. Both public investors are serious about HavenCo, complete with its dicier aspects. "I think it's a great project and I hope to see it test some of the edges of our geopolitical economy," says Ito. "The idea has great potential to force governments and other organizations to look at issues surrounding the regulation of commerce and the Internet."

Freedman says he's fully on board and enthused about the project. "If this was just about secure colocation, I wouldn't be investing," he says. "I have a firm belief that countries that encourage and foster open communication will prosper. Those that don't, won't. I see the establishment of a company to focus on the data haven aspect as an important first step. There is idealism involved. This is not strictly economic."

As the principals sketch it out, HavenCo will succeed because it has an unbeatable two-pronged business plan. First, it will operate as a traditional colocation facility — that is, a company that rents space to store servers and provides Internet connections to companies' computers and servers. Colocation is a multibillion-dollar-a-year business currently dominated by outfits like Santa Clara, California-based Exodus Communications, which builds large, earthquake-proof buildings with redundant power supplies, speedy Internet connections, and rows and rows of equipment racks housed in a secure setting. These enterprises put a premium on security, because that's exactly what clients demand. Last spring I visited an Exodus facility in Santa Clara, and my guide proudly pointed out the multiple video cameras, bulletproof glass, and palmprint readers used to verify the identity of people coming to service their equipment. Business is booming: Exodus earned $134 million during the first three months of 2000, a 32 percent increase over the previous quarter.

Nevertheless, Lackey believes HavenCo can do the job better. "Exodus looks secure, but it isn't," he insists, comparing it to a walled city that's protected against outsiders but not insiders.

Neither customers nor computers entering Exodus are physically searched or x-rayed, he says, so it would be possible to smuggle in a bomb or simply walk in and shut off the power.

HavenCo won't have these vulnerabilities, Lackey says, because even its customers won't be allowed to visit Sealand or to provide their own equipment. Instead, HavenCo will offer a range of standardized, preconfigured machines, purchased directly from the manufacturer and installed by HavenCo employees. "For us," says Lackey, "security means ensuring customers that their data will be safe from anyone and everyone, even themselves and our own employees."

It also means a willingness to laugh off legal challenges, which is part two of the master plan. For people wanting more than just colocation — who salivate over the tangy protections that a real data haven allows — HavenCo is ready to serve. Having spent time working in Anguilla, Lackey went away unimpressed, because a company operating there can still be shut down by court order if the local government decides to intervene. "Among the things that are illegal in Anguilla are pornography and any type of gambling," he sniffs. "As it stands today, Anguilla is useful only for incorporating nonresident companies and relaxing on the beach."

HavenCo will allow for gambling, pyramid schemes, adult porn, subpoena-proof email, and untraceable bank accounts. But not everything will fly. In addition to the spam and child-porn ban, corporate cybersaboteurs are forbidden. The reason, says Jo Hastings, HavenCo's chief marketing officer, is a policy dictated by Avi Freedman: Don't do anything that would inspire law enforcement officials or ISPs to shut down HavenCo's mainland Internet connections. "We will reserve the right to drop any Web site or service that would threaten our access to the Net," Hastings says.

Still, it's obvious from Lackey's gung-ho pronouncements that HavenCo will stand tough when clients need it most. Consider a real-life example from the mid-'90s, when the Church of Scientology convinced Finnish police to raid the home of a Helsinki resident, who was hosting an anonymous remailer service, anon.penet.fi. (See "alt.scientology.war," Wired 3.12, page 172.) The Scientologists wanted to know who was posting church documents on the Internet. The police showed up at the host's door and forced him to give up the name. If that remailer service had been located on Sealand, the Sealanders simply would not have complied.

But what if the church sent in a private gunboat and demanded the data? "This is how we'd deal with any battle group threatening to destroy us over a server," says Lackey, emphasizing Sealand's foursquare commitment to customer satisfaction. "We'd power off the machine, optionally destroy it, possibly turn over the smoking wreck to the attacker, and securely and anonymously refund payment to the owner of the server."

Two hours from Sealand, the water turns muddy and starts to get rough. The North Sea forecast calls for a very windy morning with rain in the afternoon; soon there are so many waves breaking over the bow that we can't see out the windows.

For "security reasons," HavenCo will mention the name of only one client: Tibet Online, the Net presence of the exiled government, which is eager to escape the clutches of China.

"I see that we are coming up against Sealand's defenses," jokes Alan Beale.

As we get closer, the water calms down and, back upstairs in the pilot's cockpit, I get my first glimpse of Sealand in the distance: Looming taller and taller as we approach, dwarfing our tiny boat, it looks like an industrial-age Stonehenge. Clearly, the structure's best defense isn't the

weather, but its height. When I visit, there are only two ways onto Sealand: landing by helicopter or getting hoisted up in a bos'n chair. I'll be taking the chair express, and, as I admit to Michael Bates, I'm nervous.

"Don't worry, you'll love it!" he roars, laughing. Beale hands me a white hard hat and a self-inflating life vest. He doesn't use these himself, but he brought them along especially for Lackey and me. "It seemed a good idea," he says gently.

High above us on the deck, two men lower what looks like the red seat from a child's swing set attached to the end of a long cable. Bill Alen takes his place on the plank of wood, grabs the ropes, and is winched 60 feet into the air and lowered onto the platform's deck.

When my turn comes I sit, hold on tight, and watch the boat fall away underneath me as I'm jerked skyward. Halfway up, the wind gains force and I'm tossed around violently. The hard hat, I realize, is there to protect my skull in case the wind bops me against the platform. It's blowing so furiously that the crew stops the winch until I stabilize. They start the motor again and soon I'm level with the railing that surrounds the deck.

"Raise your legs!" somebody shouts. I do, the crane swings around, and I'm momentarily suspended a few feet over the deck. I jump down and come face-to-face with a menacing sight: Sealand's 3.7-inch antiaircraft gun. It's covered with rust and will never fire again, but it seems like an apt symbol of the micronation's defiant future.

Not to mention its certifiably defiant past: Sealand wouldn't be what it is today without the hotspur energies of Roy Bates, who rose to the rank of major in the British army, fought in North Africa, Sicily, and Italy, and was wounded in action several times. After the war, he started various enterprises, including an import-export business, a wholesale meat business, and a 30-boat fishing fleet.

In 1965, the Bates family embarked on a project that Joan cheerfully describes as "pioneering commercial radio." Others called it pirate radio, because at the time the BBC was the only licensed broadcaster in England. Inspired in part by the success of another radio pirate, and ignoring the law, Roy set up a station on Fort Knock John, one of the abandoned WWII sea forts where he started broadcasting music and advertisements.

Called Radio Essex, the station's 5-kilowatt broadcast blanketed roughly a quarter of England. But the British government wasn't a fan: Bates received a summons in September 1966 for operating a transmitter without a license. Unfortunately for him, he had picked a tower that was just inside England's territorial limit, which was then set at 3 miles out from the coast. He was fined £100 and forced to shut down.

Roy wouldn't make the same mistake again. On Christmas Eve that year, he and Michael, 15 at the time and home from boarding school, dismantled their station and hauled everything to Roughs Tower, which was 6 miles out and therefore beyond the existing territorial limit. There wasn't much the British government could do to stop them, but the military did blow up another fort that stood beyond the 3-mile boundary, to prevent a similar takeover there.

A few months later, Roy and Joan were out with friends in a local pub. Joan mentioned casually that she wanted to have "a flag and some palm trees" to go with the "island" her husband had won for her. Their friends started listing all the things Roy and Joan could do with a

sovereign property. Roy hired an attorney to do further research, and learned that a loophole in international law left room for the Bates family to claim Roughs Tower as its own.

"It's called dereliction of sovereignty," explains Michael. "We took over the sovereignty that the British government had derelicted."

On September 2, 1967, Roy proclaimed the independence of Sealand. He pegged the country's currency to the US dollar, minted gold and silver coins, issued passports, and printed a series of stamps honoring great discoverers like Christopher Columbus and Sir Walter Raleigh.

Britain basically ignored the "country" until 1968, when, in a move that helped force the sovereignty issue, Michael fired warning shots at workmen who were servicing a navigational buoy near the platform. The next time Michael and Roy set foot on British soil, they were promptly arrested for weapons violations. But in October of that year, a British court acquitted them, ruling that since Sealand was "about 3 miles outside territorial waters," the Crown's firearms laws didn't apply there. The authorities, perhaps sensing that an embarrassing precedent was taking shape, decided not to appeal.

The British government extended its territorial limit to 12 miles in 1987, but Sealand has been allowed to plod on. Over the years, other legal cases have seemed to bolster the Bateses' sovereignty claim, though the government's stance is still nonrecognition. In 1984, the British Department of Health and Social Security issued a written ruling that Michael Bates did not have to pay his national health insurance for the periods he resided on Sealand. In 1990, Sealand once again fired shots at a boat that came too close. Local authorities investigated, but the matter was quickly dropped.

Sealand itself was never used for pirate broadcasting, due to changes in English law and a broadcasting environment that caused Roy to lose interest in pirate radio by the late '60s. Roy looked around for outside investment in the '70s and '80s, but little came of it except misadventure. Michael says that a number of "undesirables" have contacted the family over the years hoping to use the place for various schemes — from setting up some sort of "pleasure island" to smuggling. Roy claimed he was approached during the Falklands War by a group of Argentineans who wanted to buy Sealand and set up camp "right on Britain's doorstep."

"Of course I sent them away," he told The Independent in 1990. "I'd never do anything that would pose a threat to the UK."

The most raucous moment in Sealand's history occurred in 1977, when the Sealanders were approached by a German and Dutch consortium of shadowy lawyers and diamond merchants.

"They wanted to be part of what we were doing, and they wanted to develop it as well," Joan recalls. "Then they asked us to go to Austria" for a meeting. Roy was wary, but Joan persuaded him, saying, "What have we got to lose?"

When Roy and Joan arrived in Austria, five men greeted them and arranged a meeting for later. The men never showed. Suspicious, Roy and Joan tried to contact Sealand. "In those days it was very difficult," says Joan. "We had no radio communication and no telephone communication. We phoned different people who worked in the area — fishermen and the Coast Guard. One of them said, 'I saw a big helicopter hovering over Sealand.' It didn't feel right."

It wasn't. Michael was at Sealand when the helicopter showed up. As he remembers it, the mystery party lowered a man who claimed to have a telex from Roy confirming that a deal had

been made. Michael didn't buy that. Then the helicopter lowered a man who whimpered that "he was sick and needed a glass of whiskey." Michael let the helicopter land, but it was all a trick. Once on the deck, the men locked Michael up without food or water for three days. He says his attackers finally put him on a Dutch fishing boat that they "controlled," took him to Holland, and left him there without a passport or money.

Michael made his way back to Southend, where he met up with Roy and Joan. They hired a helicopter (and a dashing pilot who'd worked on a few James Bond flicks), assembled some men, and set out to recapture their country. When they arrived, Michael, shotgun in hand, slid down a rope and fired a shot — apparently by accident — and the intruders surrendered.

Swashbuckling stuff. But as the Bates admit, life on Sealand hasn't always been a thrill, and in recent years the tiny country has been sliding into obscurity. Michael lives in Southend, where he runs his business. Roy spent most of the '90s living on Sealand by himself, ready to defend its sovereignty with rifle and shotgun. Joan, afflicted with arthritis, retired to Southend, keeping in touch with Roy by cell phone. All these changes have made Sealand more than a little depressing: a geriatric experiment in nation-building, doomed to die a slow death, beaten into the sea by wind and waves.

And then came the cypherpunks.

The idea for a data haven has been around in science fiction for a while," says Sean Hastings, HavenCo's 32-year-old CEO. John Brunner's 1975 novel, *The Shockwave Rider*, features a communications haven that is invulnerable to the US government. More recently, Neal Stephenson's 1999 novel, *Cryptonomicon*, is the story of a fictional data haven on a Pacific atoll, unbreakable codes, and a brilliant protagonist coincidentally named Avi. HavenCo's founders say their inspiration didn't come from a novel, but from a chance meeting at a financial cryptography conference held in 1998.

Sean Hastings dropped out of the mathematics undergraduate program at the University of Michigan in 1989 with one semester to go because he didn't care to meet his humanities requirements. He spent eight years kicking around New York and San Francisco, where he played poker and did some programming. By 1998, he and Jo were living in New Orleans, where he wrote order-entry and automated voice-response software for legal sports-betting operations, while Jo did market studies for riverboat and tribal casinos all over the US. One day they got a call from a group of gamblers Sean knew in New York. The gamblers said they wanted to set up their own touch-tone sports-betting system — but this one would be offshore.

"They were looking for people who knew computers and knew the gambling industry," Sean says. "We said, 'That sounds fun.' So we went all through the Caribbean — went to various places — and then made our recommendation."

Sean and Jo decided that the combination of cheap telephone rates, high tech infrastructure, and easy regulations made Costa Rica an ideal spot. "Then we were told that there was this 'Cousin Bob,' and he said, 'Go to the Dominican Republic,'" and so Costa Rica was out. In the end, Cousin Bob screwed things up by insisting that the operation be headquartered at his favorite resort, which had lousy telephone connections. Eventually the project fell apart.

The Hastingses had already put their stuff in storage, rented out their New Orleans home, and bought plane tickets, so they decided to go to the Caribbean anyway. They contacted Vince Cate and Bob Green, two expatriates and high tech entrepreneurs on Anguilla, a hot spot for foreign businesses eager to take advantage of the country's tax haven status. (See "Plotting Away in Margaritaville," Wired 5.07, page 140.)

"Vince and Bob were really excited that two other people with computer knowledge might come to Anguilla," recalls Sean, who partnered with Cate on a secure payment firm. Cate, who eventually bought out Sean's share of the company and remains on amiable terms, adds that while the HavenCo idea sounds risky, he thinks Sean and Lackey might be able to pull it off.

Anguilla turned out to be a lousy location for running offshore data services. The government prohibits gambling and pornography — even on Internet servers. Sean ended up quitting because he couldn't get a work permit, but not before he found time to attend that year's Financial Cryptography Conference, an annual event that attracts bankers and cypherpunks. There, he and Jo met Ryan Lackey and Sameer Parekh.

The four decided that running Internet services from an offshore location was a fundamentally sound notion, but that Anguilla was all wrong. They needed a place with no laws regulating the Internet, cryptography, finance, or labor. Their idea was to find a small nation — some place like Tonga — whose government could recognize the wisdom of setting up a "free Internet zone."

But where? After the conference, Sean came across *How to Start Your Own Country*, a 1984 book about "new-country projects" by fringe-history buff Erwin S. Strauss. Over the years, various people have made stabs at creating a new nation out of thin air — some people have tried to do it on existing-but-unclaimed land masses, others have hatched far-fetched plans like building artificial islands and tethering them to sea mounts. Strauss catalogs them all. His book's cover shows a picture of Prince Roy and Princess Joan standing on the deck of Sealand, which he describes as "perhaps the most successful new-country venture known."

The Sealanders are arming themselves for self-defense: Plans call for "50-caliber heavy machine guns, 5.56 automatic rifles, and 12-gauge shotguns."

Sean and Jo went back to the United States intrigued by Sealand. In July 1999, Sean sent an appropriately statesmanlike email — addressed to "the royal family of Sealand" — in which he invited Sealand to participate in "a data haven project which seeks to locate servers in as many different free information jurisdictions and extranational areas as possible."

The response came four days later from Michael Bates, who was primed for a meeting, but, as a self-described "computer philistine," wanted to know more. Sean and Michael started swapping email. At the same time, Sean studied the history of Sealand and its pirate radio past. "I told Michael we were basically doing pirate Internet, which meant doing whatever people want to do, without government restrictions."

That fall, negotiations started in earnest with a face-to-face meeting involving Michael, Ryan, Sean, and Jo. What emerged was an arrangement in which the Bateses would receive an initial payment of $250,000 in cash and stock for leasing Sealand to HavenCo. And included in the deal was an option to purchase the platform at some point in the future. The Bates family

members would continue to provide for Sealand's security and contribute their expertise to the endeavor. Things moved quickly after that. By this February, HavenCo had its first investor.

In March, Sean and Jo Hastings packed their possessions into a shipping container and sent it to the Sealand platform. With more than a million dollars in first-round funding — and $2.5 million more in the pipeline — they've been slowly transforming the dingy hulk into a high tech facility. The plan is to relocate there permanently by early summer, so they've been sprucing things up with creature comforts, including exercise machines, a satellite TV receiver, DVD players, and a library.

Michael Bates and Ryan Lackey, meanwhile, have been assembling new hoists for lifting heavy objects onto Sealand's deck, bringing in generators, building a fuel tank large enough to hold a year's supply of diesel, and setting up the machine rooms in the platform's cylinders.

To be sure, the old fort needs work. During my visit, Lackey and I take a quick tour. Lackey wanders around exhibiting both awe and surprise — this is his first visit, and Sealand is smaller than he expected. A steep staircase leads down each cylinder, making it difficult to imagine bringing computers in and out. Each of the seven floors in each cylinder is actually a single concrete room, 22 feet in diameter, without storage areas or even electrical outlets. In many rooms, lighting is provided by a single bulb. The south cylinder's rooms are almost completely empty. The north cylinder contains a generator, a machine shop, and a lot of junk — mostly scrap metal.

HavenCo will start by renovating the cylinders and packing them full of computer equipment and racks. Heavier stuff like generators will sit on deck. The cylinders — the plan is to fill the south one first — are already equipped with "blast doors" to withstand explosive charges.

Internet connectivity will come from a combination of fiber, microwave links, and satellite connections. The links will carry data from Sealand to London's Telehouse and the Amsterdam Internet Exchange — two colocation providers where HavenCo itself has already rented several racks of equipment space and installed high-powered routers from Juniper Networks. At the exchanges, HavenCo can easily purchase "transit" — basically, a promise from one Net provider to another to carry its packets to their destinations — from practically any provider in Europe.

Sealand's Net connection will consist of a trio of high-speed data pipes. The first will be the satellite link — significantly slower and with a higher latency than a terrestrial connection, but a useful backup all the same. This was installed in mid-May. The second, slated for mid-June, will consist of a pair of 155-Mbps microwave links operated by Winstar Communications, which will send the data across the water to the English coast, where a line leased from British Telecom will take it to Telehouse. The third link will be a ring of high-speed fiber-optic cables installed by Flute, a UK-based corporation that builds undersea optical cable rings and then sells the fiber to its customers. According to Avi Freedman, the cable from Telehouse to the shore should be installed by June, and the fiber to the platform will be in place by September.

Obviously, any equipment located in England or the Netherlands could open up HavenCo to legal action in those countries, maybe even forcing a clampdown on its terrestrial links. But HavenCo's execs don't seem particularly worried. The important point, says Sean Hastings, is that HavenCo won't be running the servers — as is the case with Exodus, HavenCo will simply

be running the colocation facility and providing the Internet connectivity. The computers on Sealand will be owned by HavenCo's customers, who are responsible for their own actions.

And even if some angry third party convinced Telehouse to cut HavenCo's link, Sealand will be rigged to instantly reroute the data. "With three satellite connections, many transit providers, and lots of peering," says Freedman, "it's going to be very hard to shut HavenCo down."

Hastings and Lackey believe they can deal with any threat to their system that might be mounted over the Internet. But physical attacks are another matter. Lackey talks tough — telling me that plans call for "50-caliber heavy machine guns, 5.56-mm automatic rifles, and 12-gauge shotguns." But so what? A handful of guns wouldn't do much against an assault by a real nation. Which raises the biggest question of all: Can Sealand really get away with this?

Only time will answer that one, but opinions are all over the map.

Great Britain continues to maintain there is no Sealand — the 1987 expansion of her territorial limit ended the whole charade. "Although Mr. Bates styles the platform as the Principality of Sealand, the UK government does not regard Sealand as a state," says Dewi Williams, a press officer with the British Consulate in New York.

The US concurs. According to a US State Department official, who declined to be identified, "There are no independent principalities in the North Sea. As far as we are concerned, they are just Crown dependencies of Britain."

Jim Dempsey, senior staff counsel at the Center for Democracy and Technology, a Washington, DC-based civil liberties think tank, says the Sealanders are living in a dream world. "Any attempt to avoid the geographical jurisdiction of governments is ultimately futile," he insists. "There are a handful of people on Sealand who, at the very least, are nationals of some country, and that country can assert jurisdiction over them — or just send someone out to arrest them. If they are violating US laws, you wouldn't send out an Exocet missile, you'd send out a Coast Guard cutter with five policemen."

Erwin Strauss, the author of *How to Start Your Own Country*, isn't so sure. He says Britain's 1987 expansion does not change Sealand's status: If Sealand was sovereign before the change was made, it should be sovereign after. You can't take away its independence just by moving the goalposts. "From a strictly legal point of view," he says, "Roy Bates was there and claimed sovereignty, so that takes precedence."

Clearly, there's a difference of opinion, but both Michael Bates and Sean Hastings are quick to point out that there is a big difference between what Britain is saying and what it is doing. "If Britain thought they had jurisdiction over Sealand, they have been ignoring serious weapons violations under British law all this time," says Hastings. "They're pretty much saying that 'Sealand is not part of our country,' because England is normally very hard on weapons."

Ultimately, this constructive ambiguity might play to Sealand's advantage. If the UK doesn't enforce laws or collect taxes on the platform, Sealand's residents can basically do as they wish as long as they don't overly anger their nearest neighbor. On the other hand, if China, Russia, or whoever sends a destroyer to shut the place down, that boat (or at least its weapons) would have to enter British territorial waters, which would likely set off a military response from the UK.

Caroline Bradley, a professor at the University of Miami School of Law who has closely studied the international statutes affecting micronation schemes, says Sealand is in a stronger position than most new micronations, whose struggles usually involve scams or libertarian bluster that don't amount to anything. Unlike all the other wannabes chronicled by Strauss, Sealand has a population — albeit a small one — and it's about to start having an economy.

"So the question is whether other countries are going to be able to exercise any jurisdiction over Sealand to shut it down," says Bradley. She expects a bumpy road. "Countries don't like data havens. They don't like any sort of secrecy, because people who want to take advantage of such secrecy must be up to no good."

Avi Freedman responds to such criticism with a smile, arguing that if the legal going gets rough, Sealand can always fall back on being a first-rate colocation facility. "Even if you factor out all the questions about jurisdiction and history, you still have a damn fine, secure colocation business with a good economic model."

Ryan Lackey's response is, well ... Ryan Lackey-like. Whatever happens, he's ready to go for it, and true to form, he's already looking ahead and thinking big. No, bigger.

"In 10 years, we'll be investing profits in turning Sealand into a larger island," he says. "It's unclear right now whether it will be a hotel/casino space or purely a larger secure colocation facility. We hope to be in operation everywhere by then ..." Everywhere?

"By then I hope any free country in the world will have a HavenCo secure facility in major cities of commerce," Lackey continues. "No doubt we'll also have servers on ships, on the moon, and on orbiting satellites. Assuming computers continue to get smaller, a single box on the moon could serve a huge bunch of customers!"

CLASS 5: CODE

Last time, we looked at governmental power exercised through law. But, as Lessig explains, law is just one modality of regulation, and government has access to others. Today, we take up software. We'll ask how government can shape—or perhaps not shape—the way the Internet works in order to make its laws "stick." Our four examples are a French law against hate speech, Chinese laws against political dissent, a Pennsylvania law against online pornography, and a (fictitious) Delaware law against spam.

Thus, today's class combines two of our big themes. On the one hand, it continues our conversation about governmental power. And on the other, it asks us to consider how power may function differently when exercised via a keyboard rather than handcuffs.

Preparation Questions

(1) Our first reading is the Goldsmith and Wu article, a condensed version of their book *Who Controls the Internet?* Let's start with the story they tell about Yahoo! Initially, it sounds a lot like the stories from last time—United States free speech values versus French hate-speech laws. But then, Cyril Houri enters the picture, tells the judge about geolocation, and the story takes a surprising turn. What is geolocation, and why does it work? How well does it work? And why did geolocation help persuade Judge Gomez to rule against Yahoo!

(2) The next important point is Yahoo!'s response to losing the lawsuit. In December of 2000, Yahoo! filed suit in federal district court in the United States for a declaratory judgment that the initial French order was unenforceable in the United States. Why not? Why wouldn't a United States court enforce a validly entered French judgment against Yahoo!? Would it ever enforce one, or was this case special?

(3) But then the story takes *another* important twist: in 2001, Yahoo! voluntarily came into compliance with the French orders. What the bleep? Why did Yahoo! give up? Does that fact tell you anything further about why HavenCo failed?

(4) This brings us to the central theoretical point that Goldsmith and Wu make: that the Internet is becoming bordered rather than borderless. What does that mean? How will the Internet in the United States differ from the Internet in France? Have you personally seen examples of the bordered Internet? Think about some of your favorite web sites.

(5) Of course, it's not just liberal democracies that want to restrict what content is available on the Internet. Turning to the Fallows article, what kinds of technologies does China use to regulate the Internet? Does it use any of Lessig's other modalities of regulation? How? What are the effects for Chinese? For foreigners in China? For the rest of the world?

(6) Keeping in mind the Chinese example and the Yahoo! example, as well as the *Gutnick* case and the Internet gambling example from last time, in addition to everything else we've discussed, what do you think about a bordered Internet? Is this a good idea or a bad one?

(7) Now, let's move from the international arena to the domestic one. I've given you *CDT v. Pappert*, a case illustrating the Dormant Commerce Clause analysis that constrains state attempts to regulate the Internet,. How does the blocking required by the Pennsylvania law compare to the kinds of Internet control required by the French court and by China? How effective would the blocking be? Would it have more or less collateral spillover on other kinds of material?

(8) The Dormant Commerce Clause analysis itself comes in three parts. A state law may not discriminate against out-of-state commerce, it must not have burdens "clearly" excessive in relation to local benefits, and it may not regulate activity taking place wholly outside the state's borders. Which of these prongs does the Pennsylvania filtering law fail, and why?

(9) As a policy matter, the Dormant Commerce Clause puts limits on state control of the Internet. Federal preemption, of the sort seen in CAN-SPAM, is another way to shape the powers of states online—by displacing their ability to regulate entirely. Compare these systems to the various possibilities we've considered internationally. Who should control the Internet?

(10) Government power again: is it greater or lesser in the Internet age? Has your answer changed since last time?

Jack Goldsmith and Timothy Wu, *Digital Borders*
LEGAL AFFAIRS (January 2006)

IN THE 1990S, MANY PUNDITS AND SCHOLARS believed that the Internet was eroding the authority of governments. The web's salient features—instant and universal communication, geographical anonymity, and decentralized routing—made it easy for computer users inside a nation to get illegal information from computers outside the nation. American college students could download copyrighted songs from servers in the South Pacific and bet on digital blackjack tables on computers in Antigua. Saudi Arabians could access porn sites in Holland, and Italians could read banned books on web pages hosted in Australia. Nations seemed unable to stop violations of local laws via the Internet.

This conception of the Internet began to crumble in April 2000, when two French antiracism organizations sued Yahoo!, the American Internet portal, in France. The groups charged Yahoo! with hosting Nazi auction sites that were accessible in France and that violated French laws against trafficking in Nazi goods.

At the time, Yahoo! was the entrance point for more Internet users than any other website. Jerry Yang, Yahoo!'s billionaire cofounder, was confident and brash—he and David Filo had chosen the company's name because, according to the company's official history, they "liked the general definition of a yahoo: 'rude, unsophisticated, uncouth.'" Obsessed with expanding the firm's market share, Yang thought governments dumb and speech restrictions dumber still. When Yahoo! received a summons from Judge Jean-Jacques Gomez of Le Tribunal de Grande Instance de Paris, a French trial court, Yang shrugged. Reflecting conventional wisdom, he believed French officials had no authority over a computer in the United States.

And if France could do nothing to stop Yahoo! in the U.S., it also seemed hard for French officials to block access to the Nazi auction sites in their country. Too many Internet communications crossed France's borders for the government to stop and screen each one. The Internet's decentralized routing system carries messages from point to point, even if some connections along the way are blocked, damaged, or destroyed. "The Net treats censorship as a defect, and routes around it," declared John Gilmore, the libertarian Internet activist who cofounded the Electronic Frontier Foundation. To keep out the Nazi pages, it appeared that

France would have needed to shut down every single Internet access point within its borders—a seemingly impossible task.

Yahoo!'s arguments were premised on the 1990s vision of a borderless Internet. Half a decade later, this vision is fast being replaced by the reality of an Internet that is splitting apart and reflecting national borders. Far from flattening the world, the Internet is in many ways conforming to local conditions. The result is an Internet that is increasingly separated by walls of law, language, and filters. This bordered Internet reflects top-down pressures from governments like France that are imposing national laws on the Internet within their borders. But it also reflects bottom-up pressures from individuals in different places who demand an Internet that corresponds to their preferences, and from the web page operators and other content providers who shape their Internet experience to satisfy these demands. . . .

JUDGE GOMEZ RULED PRELIMINARILY IN MAY 2000 that Yahoo!'s U.S. websites violated French law, and he ordered the company "to take all necessary measures to dissuade and make impossible" visits by French web surfers to the illegal Yahoo! Nazi auction sites on yahoo.com. Jerry Yang was dismissive. "We are not going to change the content of our sites in the United States just because someone in France is asking us to do so," he said. "Asking us to filter access to our sites according to the nationality of web surfers is very naïve."

Yang's defiance reflected turn-of-the-century assumptions about the Internet's architecture. Internet protocol addresses (each computer's Internet ID), Internet domain names (such as mcdonalds.com or cnn.com), and e-mail addresses were not designed to indicate the geographical location of computers on the Net. These architectural "facts" meant that most users of 1990s Internet technology did not know where their e-mail messages and web pages were being viewed, and thus what laws in which nations they might be violating. Yahoo! said that it didn't know where its users were, and which laws it should comply with.

Worse, if France could govern Yahoo! in America, every other nation could as well. And this raised the worrying possibility that Internet firms and users, confronted with a bevy of conflicting national laws, might begin to comply with the strictest among them in order to avoid legal jeopardy. "We now risk a race to the bottom," predicted Alan Davidson of the Center for Democracy and Technology, in which "the most restrictive rules about Internet content—influenced by any country—could have an impact on people around the world."

THE SPECTER OF CONFLICTING NATIONAL LAWS applying to every Internet transaction might have given Yahoo! the edge at trial, had it not been for the unlikely intervention of Cyril Houri, a Frenchman then working in New York's Silicon Alley. On a trip home to Paris in 1999, Houri made a discovery that upended his career as a software engineer, not to mention conventional thinking about the Internet. Staying in his parents' apartment, he turned on his laptop after dinner to check his e-mail. As the computer came on, Houri saw the portal he was used to seeing in New York. Blinking cheerfully at the top of his screen was a banner advertisement for an American flower delivery service, accompanied by a 1-800-flowers number usable only in the U.S.

In that moment, Houri realized that the Internet did not point inexorably toward the flattening of frontiers. He saw that, to the contrary, a borderless flower-delivery service made no sense at all. And he grasped that people would pay for software that took the boundaries of the real world and re-created them on the Internet, so that flower deliverers and a thousand other e-

tailers would know where their customers were. There would be big money, he thought, in a technology that prevented people outside America's borders from seeing the American ad, and that substituted a French ad for a French audience and a German ad for a German one. The same technology would allow news and entertainment sites to segment their content according to the whereabouts of their audiences. All it would take was a program to pinpoint the physical location of users. So Houri founded a dot-com, Infosplit, devoted to doing just that.

Ever since the Net became commercialized in the mid-1990s, Internet firms had tried, with varying degrees of success, to discover the geographical identity of their customers. The web's omnipresent "choose a country" links are one way. Another is to ask users to type in an area code or send geographical identification (such as a driver's license) by fax or mail before allowing access to a page. Yet another is to check the address associated with a credit card as proof of geographical identification. But these techniques are sometimes unreliable and, worse, they're time-consuming. "The entire point of the Web is to bring you information simply and quickly," thought Sanjay Parekh, the founder of the geo-ID firm Digital Envoy, during an "a-ha!" experience similar to Houri's. "Why do I have to scroll through dozens of countries before accessing the site? Surely there has to be a way for [the site] to recognize where I am."

In the past decade, Infosplit, Digital Envoy, and half a dozen other firms set out to make geographical identification on the Net easy, reliable, and invisible. Instead of requiring Net users to take steps to reveal or prove their location, they devised a way to identify a user's location using the very features of Internet architecture that supposedly defied geography.

IP addresses (like "192.168.0.55") don't readily reveal a computer user's physical location. But a savvy user can determine that location by sending "tracing" packets over the Internet. These packets report a list of computers through which they travel, much as a car driving along a network of highways collects a receipt at each toll. Just as a car's origin can be determined by looking at these receipts, computers can examine the path of these packets to figure out the computers closest to the originator and recipient of any communication of the Net. This information can then be cross-checked against other IP databases that offer different clues about the geographical location of almost every computer connected to the Internet. When the databases are cross-referenced and analyzed, the location of Internet users can be determined with over 99 percent accuracy at the country level.

Internet geo-identification services are still nascent, but they are starting to have effects on e-commerce. Online identity theft in the U.S. causes firms and consumers to lose billions of dollars each year. Geo-ID is helping to solve this problem by identifying when stolen credit card numbers are used on the Net from locations like Russia, the home of many such scams. It is also improving Internet advertising, as Houri and Parekh envisioned, by making it easier to display ads geared to local conditions. And it is speeding the delivery of electronic data, allowing firms to deliver content from the closest "cache" website without having to ask the consumer where he is.

Finally, and potentially most important, these technologies are starting to enable the geographical zoning of entertainment. An important hurdle to the distribution of entertainment on the Net has been that certain material cannot lawfully be viewed in certain places. Geo-ID technologies can help to solve this problem by ensuring that online movies, web gambling sites, software programs, and other digital products do not enter countries where they are illegal. In other words, the software designed to respond to the local demands of consumers can also be used to help ensure compliance with different laws in different places.

FOLLOWING JUDGE GOMEZ'S MAY 2000 PRELIMINARY RULING, Cyril Houri contacted the plaintiff's lawyer, Stephane Lilti, and told him that his software could identify and screen Internet content on the basis of its geographical source. Houri was invited to Paris where he showed Lilti how his software worked. When the plaintiff's legal team saw what it reported, they were astonished. Yahoo!'s servers, which the firm had claimed were protected by the First Amendment to the U.S. Constitution, were actually located on a website in Stockholm. Yahoo! had placed a constantly updated "mirror" copy of its U.S. site in Sweden to speed access to the site in Europe.

When the trial resumed in July 2000, Yahoo!'s lawyers reiterated that it was impossible to identify and filter out French visitors to the firm's U.S.-based websites. Lilti responded by explaining how Houri's geo-location technology showed that Yahoo! auctions in France were not coming from servers in the U.S. Suddenly, the assumption that every web page was equally accessible to every computer user everywhere in the world seemed wrong. If Yahoo! could direct content to French users from Swedish servers, it could potentially identify users by geography and, if it liked, it could screen them out.

After receiving additional expert testimony about the feasibility of geographical screening, Gomez issued a final decision in November 2000, reaffirming that Yahoo! had violated French law by allowing Nazi goods to appear for sale on web pages in France. Gomez determined that the French court had power over Yahoo! and its servers because the company had taken conscious steps to direct the prohibited Nazi auction pages into France. He pointed out that Yahoo! greeted French visitors to its U.S. website with French-language advertisements. This showed that Yahoo! was tailoring content for France and that, to some extent, it could identify and screen users by geography. Acknowledging that 100 percent blocking was impossible, the court ordered Yahoo! to make a reasonable "best effort" to block French users.

At first, Yahoo! threatened to ignore Gomez's decision. But the company had a problem: its assets in France, including income from its French subsidiary, were at risk of seizure. In January 2001, Yahoo! abruptly surrendered. It pulled all Nazi materials from its auction sites, announcing that it would "no longer allow items that are associated with groups which promote or glorify hatred and violence to be listed on any of Yahoo!'s commerce properties." The company claimed that it was motivated by bad publicity from the Nazi auctions and not the French ruling. "Society as a whole has rejected such groups," said a Yahoo! spokesperson. But the timing and threat of French sanctions suggested that Yahoo!'s will had been broken.

YAHOO!'S CAPITULATION SHOWS WHY YANG AND SO MANY OTHERS were wrong to believe that nations could not control the local effects of Internet communications originating from outside their borders. Using powers of coercion similar to those France wielded against Yahoo!, nations can exercise control over the Internet experience within their borders. They do so by threatening the local people, equipment, and services that enable local Internet users to consume illegal communications. Government action against such local intermediaries makes it harder for users to obtain content from, or transact with, the law-evading content providers abroad.

Underneath the mists and magic of the Internet lies an ugly physical transport infrastructure: copper wires, fiber-optic cables, and the specialized routers and switches that direct information from place to place. The physical network is a local asset owned by phone companies, cable companies, and other Internet service providers that are already some of the

most regulated companies on earth. This makes ISPs the most important and obvious focal points of Internet control. For example, Germany, France, and England require local ISPs to screen out unwanted content from abroad once they are notified of its existence. But the true champions of information-transport control are found in China, which from the beginning maintained rigid control of every element in the Internet transport pipeline.

Information intermediaries are another ripe target of government control. Google frequently complies with requests to remove specified pages from its search results, usually because of alleged copyright or trademark infringements. Many of these pages are located on servers outside the United States, beyond the direct control of U.S. law. But the government, or those invoking its laws, can block the offshore content provider by going after the local search engine instead. Other countries are much more aggressive than the U.S. in using search engines to block unwanted context.

Financial intermediaries are yet another way that governments control unwanted offshore Internet flows. In response to the rise of web gambling services in the Caribbean, U.S. enforcement officials focused their attention on local financial intermediaries that help Americans ante up. In 2002, New York State Attorney General Eliot Spitzer used threats of prosecution to convince every major American credit card provider and online payment system (like PayPal) to stop honoring web gambling transactions. "With this agreement, we will cut off an enormous line of credit that was a jackpot for illegal offshore casinos," Spitzer proclaimed. And the technique seemed to work pretty well, driving half of Antiguan web gambling firms out of business, and, in the words of the Antiguan prime minister, leaving a "significant, negative impact upon the [Antiguan] economy."

Nations are using these and many other techniques of local coercion to control the Internet, including communications on it from abroad. These techniques are not perfect. Some determined web gamblers, for example, are wiring money from local banks to offshore banks—a strategy that will set off a new round of government responses. But such regulatory adjustments are as old as law itself. The law need not be completely effective to be adequately effective. All the law aims to do is to raise the costs of the activity in order to limit that activity to acceptable levels. Government regulation works by cost and bother, not by hermetic seal.

THE ENFORCEMENT OF NATIONAL LAWS in cases like Yahoo! Inc. and Yahoo France, and increasing consumer demand for Internet products tailored to local conditions, mean that what we once called a global network is becoming a collection of nation-state networks—networks linked by the Internet protocol, but for many purposes separate.

The bordered Internet is widely viewed to be a dreadful development that undermines the great network's promise. But the Net's promise was not fulfilled by the 1990s vision of an Internet dominated by the English language and the idiosyncratic values of the American First Amendment. People who use the Internet in different places read and speak different languages, and they have different interests and values that content providers want to satisfy. An Internet that accommodates these differences is a more effective and useful communication tool than one that does not.

People in different places, for example, disagree about what types of information they deem harmful. These differences are reflected in different national laws, and government officials charged with enforcing national values must enforce these laws, as cases like Yahoo! make clear.

"Every jurisdiction controls access to some speech . . . but what that speech is differs from jurisdiction to jurisdiction," explained Lawrence Lessig and Paul Resnick in a 1999 law review article. "What constitutes 'obscene' speech in Tennessee is permitted in Holland; what constitutes porn in Japan is child porn in the United States; what is 'harmful to minors' in Bavaria is Disney in New York."

France's ban on pro-Nazi speech is a reaction to its occupation by and flirtation with Nazi Germany during World War II, and its related belief that a person's right to be free from threatening and degrading speech trumps the right to voice one's political ideas, however harmful. The U.S., influenced by a very different history and tradition, takes a different view. These dramatically different attitudes toward proper speech among mature democracies reflect important differences among the peoples that populate these countries—differences in culture, history, and tastes that are legitimately reflected in national laws.

To understand the virtues of a bordered Internet, consider the opposite: an Internet dominated by a single global law. When you choose a single rule for six billion people, odds are that several billion, or more, will be unhappy with it. Is the American approach to Nazi speech right, or is the French variant? To what degree should gambling and pornography be allowed? Should data privacy be unregulated, modestly regulated, or heavily regulated? A single answer to these and thousands of other questions would leave the world divided and discontented.

SOON AFTER YAHOO!'S LEGAL DEFEAT IN FRANCE, the Chinese government insisted, as a condition of access to Chinese markets, that Yahoo! filter materials deemed harmful or threatening to the Communist Party's rule. Yahoo! agreed to China's demands, and by 2005, the company that was recently the darling of the Internet free-speech movement had become an important agent of thought control for the Chinese government. Yahoo! today provides Chinese citizens with a full suite of censored products. Its Chinese search engines do not return full results, but block sites deemed threatening to the public order by the Chinese authorities. Yahoo!'s popular chat rooms feature software filters designed to catch banned phrases like "multi-party elections" or "Taiwanese independence." The company also uses a team of human censors who monitor chat room conversations and report the most flagrant offenders to the Chinese authorities.

China and other authoritarian nations represent the downside of the bordered Internet. But technologies of control in China are essentially the same technologies designed to satisfy consumer demand for geographically tailored Internet products. And as the Yahoo! case shows, governments in democratic states are using these technologies to respond to entirely appropriate constituent demands for protection from unwanted Internet harms. Technologies of control designed to serve legitimate and desired ends can rarely be limited to those ends, and will often be co-opted for illegitimate purposes. The more important lesson is that the Internet is not, as many in the 1990s believed, an unstoppable technological juggernaut that will overrun the old and outdated determinants of human organization. To the contrary, the Internet itself is taking on the characteristics—good and bad—of the governments and people beneath it in different parts of the world.

What does Jerry Yang think of these developments? "To be doing business in China, or anywhere else in the world, we have to comply with local law," explained the one-time champion of Internet freedom. "I do not like the outcome of what happens with these things,"Yang said, "but we have to follow the law."

James Fallows, *The Connection Has Been Reset*
THE ATLANTIC (March 2008)

Many foreigners who come to China for the Olympics will use the Internet to tell people back home what they have seen and to check what else has happened in the world.

The first thing they'll probably notice is that China's Internet seems slow. Partly this is because of congestion in China's internal networks, which affects domestic and international transmissions alike. Partly it is because even electrons take a detectable period of time to travel beneath the Pacific Ocean to servers in America and back again; the trip to and from Europe is even longer, because that goes through America, too. And partly it is because of the delaying cycles imposed by China's system that monitors what people are looking for on the Internet, especially when they're looking overseas. That's what foreigners have heard about.

They'll likely be surprised, then, to notice that China's Internet seems surprisingly free and uncontrolled. Can they search for information about "Tibet independence" or "Tiananmen shooting" or other terms they have heard are taboo? Probably—and they'll be able to click right through to the controversial sites. Even if they enter the Chinese-language term for "democracy in China," they'll probably get results. What about Wikipedia, famously off-limits to users in China? They will probably be able to reach it. Naturally the visitors will wonder: What's all this I've heard about the "Great Firewall" and China's tight limits on the Internet?

In reality, what the Olympic-era visitors will be discovering is not the absence of China's electronic control but its new refinement—and a special Potemkin-style unfettered access that will be set up just for them, and just for the length of their stay. According to engineers I have spoken with at two tech organizations in China, the government bodies in charge of censoring the Internet have told them to get ready to unblock access from a list of specific Internet Protocol (IP) addresses—certain Internet cafés, access jacks in hotel rooms and conference centers where foreigners are expected to work or stay during the Olympic Games. (I am not giving names or identifying details of any Chinese citizens with whom I have discussed this topic, because they risk financial or criminal punishment for criticizing the system or even disclosing how it works. Also, I have not gone to Chinese government agencies for their side of the story, because the very existence of Internet controls is almost never discussed in public here, apart from vague statements about the importance of keeping online information "wholesome.")

Depending on how you look at it, the Chinese government's attempt to rein in the Internet is crude and slapdash or ingenious and well crafted. When American technologists write about the control system, they tend to emphasize its limits. When Chinese citizens discuss it—at least with me—they tend to emphasize its strength. All of them are right, which makes the government's approach to the Internet a nice proxy for its larger attempt to control people's daily lives.

Disappointingly, "Great Firewall" is not really the right term for the Chinese government's overall control strategy. China has indeed erected a firewall—a barrier to keep its Internet users from dealing easily with the outside world—but that is only one part of a larger, complex structure of monitoring and censorship. The official name for the entire approach, which is ostensibly a way to keep hackers and other rogue elements from harming Chinese Internet users, is the "Golden Shield Project." Since that term is too creepy to bear repeating, I'll use "the

control system" for the overall strategy, which includes the "Great Firewall of China," or GFW, as the means of screening contact with other countries.

In America, the Internet was originally designed to be free of choke points, so that each packet of information could be routed quickly around any temporary obstruction. In China, the Internet came with choke points built in. Even now, virtually all Internet contact between China and the rest of the world is routed through a very small number of fiber-optic cables that enter the country at one of three points: the Beijing-Qingdao-Tianjin area in the north, where cables come in from Japan; Shanghai on the central coast, where they also come from Japan; and Guangzhou in the south, where they come from Hong Kong. (A few places in China have Internet service via satellite, but that is both expensive and slow. Other lines run across Central Asia to Russia but carry little traffic.) In late 2006, Internet users in China were reminded just how important these choke points are when a seabed earthquake near Taiwan cut some major cables serving the country. It took months before international transmissions to and from most of China regained even their pre-quake speed, such as it was.

Thus Chinese authorities can easily do something that would be harder in most developed countries: physically monitor all traffic into or out of the country. They do so by installing at each of these few "international gateways" a device called a "tapper" or "network sniffer," which can mirror every packet of data going in or out. This involves mirroring in both a figurative and a literal sense. "Mirroring" is the term for normal copying or backup operations, and in this case real though extremely small mirrors are employed. Information travels along fiber-optic cables as little pulses of light, and as these travel through the Chinese gateway routers, numerous tiny mirrors bounce reflections of them to a separate set of "Golden Shield" computers. Here the term's creepiness is appropriate. As the other routers and servers (short for file servers, which are essentially very large-capacity computers) that make up the Internet do their best to get the packet where it's supposed to go, China's own surveillance computers are looking over the same information to see whether it should be stopped.

The mirroring routers were first designed and supplied to the Chinese authorities by the U.S. tech firm Cisco, which is why Cisco took such heat from human-rights organizations. Cisco has always denied that it tailored its equipment to the authorities' surveillance needs, and said it merely sold them what it would sell anyone else. The issue is now moot, since similar routers are made by companies around the world, notably including China's own electronics giant, Huawei. The ongoing refinements are mainly in surveillance software, which the Chinese are developing themselves. Many of the surveillance engineers are thought to come from the military's own technology institutions. Their work is good and getting better, I was told by Chinese and foreign engineers who do "oppo research" on the evolving GFW so as to design better ways to get around it.

Andrew Lih, a former journalism professor and software engineer now based in Beijing (and author of the forthcoming book *The Wikipedia Story*), laid out for me the ways in which the GFW can keep a Chinese Internet user from finding desired material on a foreign site. In the few seconds after a user enters a request at the browser, and before something new shows up on the screen, at least four things can go wrong—or be made to go wrong.

The first and bluntest is the "DNS block." The DNS, or Domain Name System, is in effect the telephone directory of Internet sites. Each time you enter a Web address, or URL—www.yahoo.com, let's say—the DNS looks up the IP address where the site can be found. IP

addresses are numbers separated by dots—for example, TheAtlantic.com's is 38.118.42.200. If the DNS is instructed to give back no address, or a bad address, the user can't reach the site in question—as a phone user could not make a call if given a bad number. Typing in the URL for the BBC's main news site often gets the no-address treatment: if you try news.bbc.co.uk, you may get a "Site not found" message on the screen. For two months in 2002, Google's Chinese site, Google.cn, got a different kind of bad-address treatment, which shunted users to its main competitor, the dominant Chinese search engine, Baidu. Chinese academics complained that this was hampering their work. The government, which does not have to stand for reelection but still tries not to antagonize important groups needlessly, let Google.cn back online. During politically sensitive times, like last fall's 17th Communist Party Congress, many foreign sites have been temporarily shut down this way.

Next is the perilous "connect" phase. If the DNS has looked up and provided the right IP address, your computer sends a signal requesting a connection with that remote site. While your signal is going out, and as the other system is sending a reply, the surveillance computers within China are looking over your request, which has been mirrored to them. They quickly check a list of forbidden IP sites. If you're trying to reach one on that blacklist, the Chinese international-gateway servers will interrupt the transmission by sending an Internet "Reset" command both to your computer and to the one you're trying to reach. Reset is a perfectly routine Internet function, which is used to repair connections that have become unsynchronized. But in this case it's equivalent to forcing the phones on each end of a conversation to hang up. Instead of the site you want, you usually see an onscreen message beginning "The connection has been reset"; sometimes instead you get "Site not found." Annoyingly, blogs hosted by the popular system Blogspot are on this IP blacklist. For a typical Google-type search, many of the links shown on the results page are from Wikipedia or one of these main blog sites. You will see these links when you search from inside China, but if you click on them, you won't get what you want.

The third barrier comes with what Lih calls "URL keyword block." The numerical Internet address you are trying to reach might not be on the blacklist. But if the words in its URL include forbidden terms, the connection will also be reset. (The Uniform Resource Locator is a site's address in plain English—say, www.microsoft.com—rather than its all-numeric IP address.) The site FalunGong.com appears to have no active content, but even if it did, Internet users in China would not be able to see it. The forbidden list contains words in English, Chinese, and other languages, and is frequently revised—"like, with the name of the latest town with a coal mine disaster," as Lih put it. Here the GFW's programming technique is not a reset command but a "black-hole loop," in which a request for a page is trapped in a sequence of delaying commands. These are the programming equivalent of the old saw about how to keep an idiot busy: you take a piece of paper and write "Please turn over" on each side. When the Firefox browser detects that it is in this kind of loop, it gives an error message saying: "The server is redirecting the request for this address in a way that will never complete."

The final step involves the newest and most sophisticated part of the GFW: scanning the actual contents of each page—which stories *The New York Times* is featuring, what a China-related blog carries in its latest update—to judge its page-by-page acceptability. This again is done with mirrors. When you reach a favorite blog or news site and ask to see particular items, the requested pages come to you—and to the surveillance system at the same time. The GFW scanner checks the content of each item against its list of forbidden terms. If it finds something it doesn't like, it breaks the connection to the offending site and won't let you download anything

further from it. The GFW then imposes a temporary blackout on further "IP1 to IP2" attempts—that is, efforts to establish communications between the user and the offending site. Usually the first time-out is for two minutes. If the user tries to reach the site during that time, a five-minute time-out might begin. On a third try, the time-out might be 30 minutes or an hour—and so on through an escalating sequence of punishments.

Users who try hard enough or often enough to reach the wrong sites might attract the attention of the authorities. At least in principle, Chinese Internet users must sign in with their real names whenever they go online, even in Internet cafés. When the surveillance system flags an IP address from which a lot of "bad" searches originate, the authorities have a good chance of knowing who is sitting at that machine.

All of this adds a note of unpredictability to each attempt to get news from outside China. One day you go to the NPR site and cruise around with no problem. The next time, NPR happens to have done a feature on Tibet. The GFW immobilizes the site. If you try to refresh the page or click through to a new story, you'll get nothing—and the time-out clock will start.

This approach is considered a subtler and more refined form of censorship, since big foreign sites no longer need be blocked wholesale. In principle they're in trouble only when they cover the wrong things. Xiao Qiang, an expert on Chinese media at the University of California at Berkeley journalism school, told me that the authorities have recently begun applying this kind of filtering in reverse. As Chinese-speaking people outside the country, perhaps academics or exiled dissidents, look for data on Chinese sites—say, public-health figures or news about a local protest—the GFW computers can monitor what they're asking for and censor what they find.

Taken together, the components of the control system share several traits. They're constantly evolving and changing in their emphasis, as new surveillance techniques become practical and as words go on and off the sensitive list. They leave the Chinese Internet public unsure about where the off-limits line will be drawn on any given day. Andrew Lih points out that other countries that also censor Internet content—Singapore, for instance, or the United Arab Emirates—provide explanations whenever they do so. Someone who clicks on a pornographic or "anti-Islamic" site in the U.A.E. gets the following message, in Arabic and English: "We apologize the site you are attempting to visit has been blocked due to its content being inconsistent with the religious, cultural, political, and moral values of the United Arab Emirates." In China, the connection just times out. Is it your computer's problem? The firewall? Or maybe your local Internet provider, which has decided to do some filtering on its own? You don't know. "The unpredictability of the firewall actually makes it more effective," another Chinese software engineer told me. "It becomes much harder to know what the system is looking for, and you always have to be on guard."

There is one more similarity among the components of the firewall: they are all easy to thwart.

As a practical matter, anyone in China who wants to get around the firewall can choose between two well-known and dependable alternatives: the proxy server and the VPN. A proxy server is a way of connecting your computer inside China with another one somewhere else—or usually to a series of foreign computers, automatically passing signals along to conceal where they really came from. You initiate a Web request, and the proxy system takes over, sending it to a computer in America or Finland or Brazil. Eventually the system finds what you want and sends

it back. The main drawback is that it makes Internet operations very, very slow. But because most proxies cost nothing to install and operate, this is the favorite of students and hackers in China.

A VPN, or virtual private network, is a faster, fancier, and more elegant way to achieve the same result. Essentially a VPN creates your own private, encrypted channel that runs alongside the normal Internet. From within China, a VPN connects you with an Internet server somewhere else. You pass your browsing and downloading requests to that American or Finnish or Japanese server, and it finds and sends back what you're looking for. The GFW doesn't stop you, because it can't read the encrypted messages you're sending. Every foreign business operating in China uses such a network. VPNs are freely advertised in China, so individuals can sign up, too. I use one that costs $40 per year. (An expat in China thinks: *that's a little over a dime a day*. A Chinese factory worker thinks: *it's a week's take-home pay*. Even for a young academic, it's a couple days' work.)

As a technical matter, China could crack down on the proxies and VPNs whenever it pleased. Today the policy is: if a message comes through that the surveillance system cannot read because it's encrypted, let's wave it on through! Obviously the system's behavior could be reversed. But everyone I spoke with said that China could simply not afford to crack down that way. "Every bank, every foreign manufacturing company, every retailer, every software vendor needs VPNs to exist," a Chinese professor told me. "They would have to shut down the next day if asked to send their commercial information through the regular Chinese Internet and the Great Firewall." Closing down the free, easy-to-use proxy servers would create a milder version of the same problem. Encrypted e-mail, too, passes through the GFW without scrutiny, and users of many Web-based mail systems can establish a secure session simply by typing "https:" rather than the usual "http:" in a site's address—for instance, https://mail.yahoo.com. To keep China in business, then, the government has to allow some exceptions to its control efforts—even knowing that many Chinese citizens will exploit the resulting loopholes.

Because the Chinese government can't plug every gap in the Great Firewall, many American observers have concluded that its larger efforts to control electronic discussion, and the democratization and grass-roots organizing it might nurture, are ultimately doomed. A recent item on an influential American tech Web site had the headline "Chinese National Firewall Isn't All That Effective." In October, *Wired* ran a story under the headline "The Great Firewall: China's Misguided—and Futile—Attempt to Control What Happens Online."

Let's not stop to discuss why the vision of democracy-through-communications-technology is so convincing to so many Americans. (Samizdat, fax machines, and the Voice of America eventually helped bring down the Soviet system. Therefore proxy servers and online chat rooms must erode the power of the Chinese state. Right?) Instead, let me emphasize how unconvincing this vision is to most people who deal with China's system of extensive, if imperfect, Internet controls.

Think again of the real importance of the Great Firewall. Does the Chinese government really care if a citizen can look up the Tiananmen Square entry on Wikipedia? Of course not. Anyone who wants that information will get it—by using a proxy server or VPN, by e-mailing to a friend overseas, even by looking at the surprisingly broad array of foreign magazines that arrive, uncensored, in Chinese public libraries.

What the government cares about is making the quest for information just enough of a nuisance that people generally won't bother. Most Chinese people, like most Americans, are

interested mainly in their own country. All around them is more information about China and things Chinese than they could possibly take in. The newsstands are bulging with papers and countless glossy magazines. The bookstores are big, well stocked, and full of patrons, and so are the public libraries. Video stores, with pirated versions of anything. Lots of TV channels. And of course the Internet, where sites in Chinese and about China constantly proliferate. When this much is available inside the Great Firewall, why go to the expense and bother, or incur the possible risk, of trying to look outside?

All the technology employed by the Golden Shield, all the marvelous mirrors that help build the Great Firewall—these and other modern achievements matter mainly for an old-fashioned and pre-technological reason. By making the search for external information a nuisance, they drive Chinese people back to an environment in which familiar tools of social control come into play.

Chinese bloggers have learned that if they want to be read in China, they must operate within China, on the same side of the firewall as their potential audience. Sure, they could put up exactly the same information outside the Chinese mainland. But according to Rebecca MacKinnon, a former Beijing correspondent for CNN now at the Journalism and Media Studies Center of the University of Hong Kong, their readers won't make the effort to cross the GFW and find them. "If you want to have traction in China, you have to *be* in China," she told me. And being inside China means operating under the sweeping rules that govern all forms of media here: guidance from the authorities; the threat of financial ruin or time in jail; the unavoidable self-censorship as the cost of defiance sinks in.

Most blogs in China are hosted by big Internet companies. Those companies know that the government will hold them responsible if a blogger says something bad. Thus the companies, for their own survival, are dragooned into service as auxiliary censors.

Large teams of paid government censors delete offensive comments and warn errant bloggers. (No official figures are available, but the censor workforce is widely assumed to number in the tens of thousands.) Members of the public at large are encouraged to speak up when they see subversive material. The propaganda ministries send out frequent instructions about what can and cannot be discussed. In October, the group Reporters Without Borders, based in Paris, released an astonishing report by a Chinese Internet technician writing under the pseudonym "Mr. Tao." He collected dozens of the messages he and other Internet operators had received from the central government. Here is just one, from the summer of 2006:

> 17 June 2006, 18:35
>
> From: Chen Hua, deputy director of the Beijing Internet Information Administrative Bureau
>
> Dear colleagues, the Internet has of late been full of articles and messages about the death of a Shenzhen engineer, Hu Xinyu, as a result of overwork. All sites must stop posting articles on this subject, those that have already been posted about it must be removed from the site and, finally, forums and blogs must withdraw all articles and messages about this case.

"Domestic censorship is the real issue, and it is about social control, human surveillance, peer pressure, and self-censorship," Xiao Qiang of Berkeley says. Last fall, a team of computer

scientists from the University of California at Davis and the University of New Mexico published an exhaustive technical analysis of the GFW's operation and of the ways it could be foiled. But they stressed a nontechnical factor: "The presence of censorship, even if easy to evade, promotes self-censorship."

It would be wrong to portray China as a tightly buttoned mind-control state. It is too wide-open in too many ways for that. "Most people in China feel freer than any Chinese people have been in the country's history, ever," a Chinese software engineer who earned a doctorate in the United States told me. "There has never been a space for any kind of discussion before, and the government is clever about continuing to expand space for anything that doesn't threaten its survival." But it would also be wrong to ignore the cumulative effect of topics people are not allowed to discuss. "Whether or not Americans supported George W. Bush, they could not *avoid* learning about Abu Ghraib," Rebecca MacKinnon says. In China, "the controls mean that whole topics inconvenient for the regime simply don't exist in public discussion." Most Chinese people remain wholly unaware of internationally noticed issues like, for instance, the controversy over the Three Gorges Dam.

Countless questions about today's China boil down to: How long can this go on? How long can the industrial growth continue before the natural environment is destroyed? How long can the super-rich get richer, without the poor getting mad? And so on through a familiar list. The Great Firewall poses the question in another form: How long can the regime control what people are allowed to know, without the people caring enough to object? On current evidence, for quite a while.

Center for Democracy and Technology v. Pappert
337 F. Supp. 2d 606 (E.D. Pa. 2004)

MEMORANDUM

I. INTRODUCTION

In February of 2002, Pennsylvania enacted the Internet Child Pornography Act, 18 Pa. Cons. Stat. §§ 7621-7630, ("the Act"). The Act requires an Internet Service Provider ("ISP") to remove or disable access to child pornography items "residing on or accessible through its service" after notification by the Pennsylvania Attorney General. It is the first attempt by a state to impose criminal liability on an ISP which merely provides access to child pornography through its network and has no direct relationship with the source of the content.

The plaintiffs are Center for Democracy and Technology ("CDT"), the American Civil Liberties Union of Pennsylvania ("ACLU"), and Plantagenet, Inc. CDT is a non-profit corporation incorporated for the purpose of educating the general public concerning public policy issues related to the Internet. The ACLU is a non-partisan organization of more than 13,000 members dedicated to defending the principles of liberty and equality embodied in the Bill of Rights. Plantagenet, Inc., is an ISP that provides a variety of services related to the Internet. Defendant is Gerald J. Pappert, Attorney General of the Commonwealth of Pennsylvania. . . .

II. PROCEDURAL HISTORY

. . . [After filing an initial complaint], plaintiffs filed a Motion for Declaratory Relief and for Preliminary and Permanent Injunctive Relief on December 12, 2003 that essentially sought the

same relief as was sought in the Complaint. A hearing on this Motion commenced on January 6, 2004. Based on an agreement between the parties, the hearing on the Motion for Declaratory Relief and Preliminary Injunctive Relief was consolidated with a trial on the merits by Order dated March 1, 2004. Because of the schedule of the Court and the parties, the trial continued over twelve non-consecutive days before it concluded with oral argument on June 23, 2004. Following the trial, the parties submitted supplemental memoranda and post-trial proposed findings of fact.

III. FINDINGS OF FACT

. . .

C. INTERNET CHILD PORNOGRAPHY ACT ("THE ACT")

48. On February 21, 2002, Pennsylvania enacted the Internet Child Pornography Act, codified at 18 Pa. Cons. Stat. § 7330 and effective in 60 days (April 22, 2002) ("the Act"). On December 16, 2002, the Act was recodified at 18 Pa. Cons. Stat. §§ 7621-7630, without change in substance.

49. The Act permits defendant or a district attorney in Pennsylvania to seek a court order requiring an ISP to "remove or disable items residing on or accessible through" an ISP's service upon a showing of probable cause that the item constitutes child pornography. The application for a court order must contain the Uniform Resource Locator providing access to the item.

50. Child pornography is defined as images that display a child under the age of 18 engaged in a "prohibited sexual act." A prohibited sexual act is defined as "sexual intercourse . . . masturbation, sadism, masochism, bestiality, fellatio, cunnilingus, lewd exhibition of the genitals or nudity if such nudity is depicted for the purpose of sexual stimulation or gratification of any person who might view such depiction."

51. The court order may be obtained on an ex parte basis with no prior notice to the ISP or the web site owner and no post-hearing notice to the web site owner.

52. Under the Act, a judge may issue an order directing that the challenged content be removed or disabled from the ISP's service upon a showing that the items constitute probable cause evidence of child pornography. A judge does not make a final determination that the challenged content is child pornography.

53. Once a court order is issued, the Pennsylvania Attorney General notifies the ISP in question and provides the ISP with a copy of the court order. The ISP then has five days to block access to the specified content or face criminal liability, including fines of up to $ 30,000 and a prison term of up to seven years.

54. According to defendant, the purpose of the Act is: "To protect children from sexual exploitation and abuse. To serve this purpose by interfering with distribution of child pornography, particularly its distribution over the Internet."

55. Government law enforcement agencies have attempted to locate and criminally prosecute persons who produce or knowingly distribute child pornography. However, a state agency in the United States cannot easily prosecute producers and distributors of child pornography because they are rarely found in that particular state and often are not found in the United States. . . .

F. IMPACT OF THE ACT ON INTERSTATE COMMERCE

210. Some ISPs were only able to implement blocking orders on a nationwide basis. Some of these ISPs communicated this fact to the OAG before the Act took effect. The OAG's Chief Information Officer, Peter Sand, recognized that implementation of the Act might extend outside of Pennsylvania, stating: "I think [the ISPs are] all distracted by their belief that they will have to make a technical distinction between [Pennsylvania] customers and their other customers. They might be technically unable to make that distinction. . . I think we may face a larger, legal problem by someone who might argue that what we are in fact doing is regulating 'stuff' outside of our geographic jurisdiction."

211. The blocking actions taken by AOL to comply with the Informal Notices were applied to AOL's entire global network and thus halted communications that took place entirely outside of Pennsylvania (and the U.S.). AOL told the OAG that it was "technologically incapable" of confining the impact of compliance with blocking orders to the Commonwealth of Pennsylvania.

212. The court order issued to WorldCom under the Act resulted in obstruction of communications on WorldCom's entire North American network. This blocking affects all WorldCom customers in the United States and Canada and some WorldCom customers located overseas. As a hypothetical, a WorldCom customer in Minnesota would not be able to access a web site located in Georgia if it was blocked as a result of WorldCom's compliance with a Pennsylvania blocking order. WorldCom informed the OAG that it was not technically feasible for it to block access only to Pennsylvania subscribers and that it would have to block access to all users of WorldCom's North American network.

213. Verizon informed the OAG about the interstate impact of blocking orders on its network. As Verizon explained, "blocking access to content or URLs accessible to Pennsylvania residents through Verizon-owned DNS servers requires Verizon also to block access to the same content and URLs by customers in other states who use these same DNS servers."

214. ISPs do not organize or design their internal networks along state boundaries, and thus it would be "extremely challenging" for an ISP to limit the impact of URL filtering to the State of Pennsylvania.

215. Even communications between Pennsylvanians are likely to be interstate communications. For example, all World Wide Web traffic of AOL's dial-up customers in Pennsylvania passes through an AOL data center located in Virginia.

IV. CONCLUSIONS OF LAW

. . .

D. INTERSTATE COMMERCE CLAUSE

Plaintiffs argue that the Act and Informal Notices violate the Commerce Clause because, given the fact that most ISP's networks cross state boundaries, the blocking orders "impose restrictions on communications occurring wholly outside of a Pennsylvania, effect an impermissible burden on interstate commerce, and risk subjecting Internet speech to inconsistent state obligations."

The Constitution grants Congress the power "to regulate Commerce . . . among the several States." U.S. Const. art. I, § 8, cl. 3. The Supreme Court has decided that the Commerce Clause

has a negative aspect, commonly called "the dormant Commerce Clause," that limits the states' power to regulate interstate commerce. "The dormant Commerce Clause prohibits the states from imposing restrictions that benefit in-state economic interests at out-of-state interests' expense." *Cloverland-Green Spring Dairies, Inc. v. Pa. Milk Mktg. Bd.*, 298 F.3d 201, 210 (3d Cir. 2002) (citing *West Lynn Creamery, Inc. v. Healy*, 512 U.S. 186, 192-93, 129 L. Ed. 2d 157, 114 S. Ct. 2205 (1994)).

The first question the Court must answer in conducting a dormant Commerce Clause analysis is "whether the state regulation at issue discriminates against interstate commerce 'either on its face or in practical effect.' If so, heightened scrutiny applies." *Id.* "On the other hand, if the state regulation does not discriminate against interstate commerce, but 'regulates even-handedly' and merely 'incidentally' burdens it, the regulation will be upheld unless the burden is 'clearly excessive in relation to the putative local benefits.'" *Id.* at 211 (quoting *Pike v. Bruce Church, Inc.* 397 U.S. 137, 142, 25 L. Ed. 2d 174, 90 S. Ct. 844 (1970)).

Plaintiffs do not argue that the Act favors in-state commerce over out-of-state commerce on its face or in practical effect. As a result, the balancing test applied in *Pike v. Bruce Church* quoted above will be applied. Plaintiffs also argue that a Act is per se invalid under the dormant Commerce Clause because it has the "practical effect" of regulating commerce occurring wholly outside state's borders.

1. Pike Balancing Test

The Act cannot survive the dormant Commerce Clause balancing test set forth in *Pike v. Bruce Church, Inc.* 397 U.S. 137, 25 L. Ed. 2d 174, 90 S. Ct. 844 (1970). Under *Pike*, if the Act is an "evenhanded regulation to effectuate a legitimate local public interest, and its effects on interstate commerce are only incidental, it will be upheld unless the burden imposed is clearly excessive in relation to local benefits." *Id.* at 142. In this case, there is a legitimate local interest — combating child pornography and sexual abuse of children — and the effects on interstate commerce are only incidental. Thus, the Court must determine if the burden imposed is clearly excessive in relation to local benefits.

The courts in *PSInet*, *Johnson*, and *Pataki* concluded that the burdens of state pornography laws were clearly excessive in relation to local benefits. *PSInet*, 362 F.3d at 240, *ACLU v. Johnson*, 194 F.3d at 1160-61, *Pataki*, 969 F. Supp. at 177-181. In fact, every federal court that examined a state law that directly regulated the Internet determined that the state law failed the *Pike* balancing test. *Id.*; but see *Ford Motor Co. v. Tex. DOT*, 264 F.3d 493, 505 (5th Cir. 2001) (distinguishing "incidental regulation of internet activities" in that case from direct regulation in *Pataki*).

This Court also concludes that the burdens imposed by the Act are clearly excessive in relation to the local benefits. Defendant claims the Act is justified by reducing the sexual abuse of children. However, defendant did not produce any evidence that the Act effectuates this goal. To the contrary, there have been no prosecutions of child pornographers and the evidence shows that individuals interested in obtaining or providing child pornography can evade blocking efforts using a number of different methods. *Id.*

Moreover, there is evidence that this Act places a substantial burden on interstate commerce. Defendant argues that the Act only burdens child pornography, which is not a legitimate form of commerce. To the contrary, the evidence demonstrates that implementation of the Act has

impacted a number of entities involved in the commerce of the Internet — ISPs, web publishers, and users of the Internet. To comply with the Act, ISPs have used two types of filtering — IP filtering and DNS filtering — to disable access to alleged child pornography. This filtering resulted in the suppression of 376 web sites containing child pornography, certainly a local benefit. However, the filtering used by the ISPs also resulted in the suppression of in excess of 1,190,000 web sites not targeted by defendant and, as demonstrated at trial, a number of these web sites, probably most of them, do not contain child pornography. The overblocking harms web publishers which seek wide distribution for their web sites and Internet users who want access to the broadest range of content possible. For example, as a result of a block implemented by AOL in response to an Informal Notice, Ms. Goldwater, a self employed documentary film maker, was unable to access a web site selling movie posters.

Based on this evidence, the Court concludes that the burden imposed by the Act is clearly excessive in relation to the local benefits. Thus, the Act must fail under the dormant Commerce Clause as an invalid indirect regulation of interstate commerce.

2. Per se Invalidity

A number of cases have invalidated state laws regulating the Internet because the laws regulated activity occurring wholly outside the state's borders or because they have had an "extraterritorial" effect. The court in *American Libraries Ass'n v. Pataki*, 969 F. Supp. 160, 177 (S.D.N.Y. 1997) invalidated a New York state law that regulated the Internet because "the nature of the Internet makes it impossible to restrict the effects of the New York Act to conduct occurring within New York. . . . Thus, conduct that may be legal in the state in which the user acts can subject the user to prosecution in New York and thus subordinate the user's home state"s policy — perhaps favoring freedom of expression over a more protective stance — to New York's local concerns." This ruling was followed in *American Booksellers Foundation v. Dean*, 342 F.3d 96 (2d Cir. 2003), *ACLU v. Johnson*, 194 F.3d 1149, 1161 (10th Cir. 1999), and cited with approval in *PSInet v. Chapman*, 362 F.3d 227 (4th Cir. 2004). As explained in *Healy v. The Beer Institute*, 491 U.S. 324, 105 L. Ed. 2d 275, 109 S. Ct. 2491 (1989), the Commerce Clause protects against "against inconsistent legislation arising from the projection of one state regulatory regime into the jurisdiction of another State." *Id.* at 337.

This Act has the practical effect of exporting Pennsylvania's domestic policies. *Pataki*, 969 F. Supp. at 174. As an example, a WorldCom witness testified that a customer in Minnesota would not be able to access a web site hosted in Georgia if an IP Address was blocked by a Pennsylvania order. The Act is even more burdensome than the legislation examined in Pataki because Pennsylvania has suppressed speech that was not targeted by the Act. Thus, a Minnesotan would be prevented from accessing a Georgia web site that is not even alleged to contain child pornography.

A number of courts have concluded that the Internet should not be subject to state regulation. *Am. Booksellers Found. v. Dean*, 342 F.3d 96, 104 (2d Cir. 2003) ("We think it likely that the internet will soon be seen as falling within the class of subjects that are protected from State regulation because they 'imperatively demand[] a single uniform rule.'"), *American Libraries Ass'n v. Pataki*, 969 F. Supp. 160, 181 (S.D.N.Y 1997) ("The courts have long recognized that certain types of commerce demand consistent treatment and are therefore susceptible to regulation only on a national level. The Internet represents one of those areas; effective regulation will require national, and more likely global, cooperation. Regulation by any single state can only result in

chaos, because at least some states will likely enact laws subjecting Internet users to conflicting obligations."). Although the Court is not prepared to rule that states can never regulate the Internet, the Act's extraterritorial effect violates the dormant Commerce Clause.

V. CONCLUSION

For the foregoing reasons, plaintiffs' Motion for Declaratory Relief and Preliminary and Permanent Injunctive Relief is granted. Pennsylvania's Internet Child Pornography Act, 18 Pa. Stat. Ann. § 7621-7630 and the Informal Notice process used by defendant to implement the Act are declared unconstitutional. Defendant is enjoined from taking any action against an ISP for failing to comply with an Informal Notice or court order under the Act. The ISPs which blocked web sites pursuant to Informal Notices and, with respect to WorldCom, a court order shall promptly remove the blocks.

An appropriate Order follows.

Spam Problem

The following problem is based in part on *State v. Heckel*, 24 P.3d 404 (Wash. 2001) and *Omega World Travel, Inc. v. Mummagraphics, Inc.*, 469 F. 3d 348 (4th Cir. 2006):

In 1998, Delaware enacted the Delaware Anti-Spam Act (DASA), which provided, in part:

> "(1) No person may initiate the transmission, conspire with another to initiate the transmission, or assist the transmission, of a commercial electronic mail message from a computer located in Delaware or to an electronic mail address that the sender knows, or has reason to know, is held by a Delaware resident that:
>
> (a) Uses a third party's internet domain name without permission of the third party, or otherwise misrepresents or obscures any information in identifying the point of origin or the transmission path of a commercial electronic mail message; or
>
> (b) Contains false or misleading information in the subject line; or
>
> (c) Does not contain the text "ADVERTISEMENT" or similar disclaimer in the subject line; or
>
> (d) Advertises the sale of any alcoholic beverage subject to the jurisdiction of the Delaware Bureau of Liquor Control.
>
> (2) For purposes of this section, a person knows that the intended recipient of a commercial electronic mail message is a Delaware resident if that information is available, upon request, from the registrant of the Internet domain name contained in the recipient's electronic mail address."

The state attempted to prosecute Jason Heckel under this statute. Here is the recitation of facts from the case in which the court considered Heckel's various constitutional and statutory objections to the prosecution:

> As early as February 1998, defendant Jason Heckel, an Oregon resident doing business as Natural Instincts, began sending unsolicited commercial e-mail (UCE), or

"spam," over the Internet.[1] In 1999, Heckel developed a 46 page on-line booklet entitled "How to Profit from the Internet." The booklet described how to set up an on-line promotional business, acquire free e-mail accounts, and obtain software for sending bulk e-mail. From June 2000, Heckel marketed the booklet by sending between 100,000 and 1,000,000 UCE messages per week. To acquire the large volume of e-mail addresses, Heckel used the Extractor Pro software program, which harvests e-mail addresses from various on-line sources and enables a spammer to direct a bulk-mail message to those addresses by entering a simple command. The Extractor Pro program requires the spammer to enter a return e-mail address, a subject line, and the text of the message to be sent. The text of Heckel's UCE was a lengthy sales pitch that included testimonials from satisfied purchasers and culminated in an order form that the recipient could download and print. The order form included the Salem, Oregon, mailing address for Natural Instincts. Charging $39.95 for the booklet, Heckel made 30 to 50 sales per month.

Heckel used one of two subject lines to introduce his solicitations: "Did I get the right e-mail address?" and "For your review—HANDS OFF!" Heckel routed[2] his spam through at least a dozen different domain names without receiving permission to do so from the registered owners of those names. For example, of the 20 complaints the Attorney General's Office received concerning Heckel's spam, 9 of the messages showed "13.com" as the initial ISP to transmit his spam. The 13.com domain name, however, was registered to another individual, from whom Heckel had not sought or received permission to use the registered name. In fact, because the owner of 13.com had not yet even activated that domain name, no messages could have been sent or received through 13.com.

1) Are these facts, if proven at trial, sufficient to convict Heckel of a violation of DASA?

2) Is DASA consistent with the Dormant Commerce Clause?

---

[1] "`Commercial electronic mail message' means an electronic mail message sent for the purpose of promoting real property, goods, or services for sale or lease." RCW 19.190.010(2). The term "spam" refers broadly to unsolicited bulk e-mail (or "`junk' e-mail"), which "can be either commercial (such as an advertisement) or noncommercial (such as a joke or chain letter)." Use of the term "spam" as Internet jargon for this seemingly ubiquitous junk e-mail arose out of a skit by the British comedy troupe Monty Python, in which a waitress can offer a patron no single menu item that does not include spam: "Well, there's spam, egg, sausage and spam. That's not got much spam in it." Because the term has been widely adopted by Internet users, legislators, and legal commentators, we use the term herein, along with its useful derivatives "spammer" and "spamming."

[2] Each e-mail message, which is simply a computer data file, contains so-called "header" information in the "To," "From," and "Received" fields. When an e-mail message is transmitted from one e-mail address to another, the message generally passes through at least four computers: from the sender's computer, the message travels to the mail server computer of the sender's Internet Service Provider (ISP); that computer delivers the message to the mail server computer of the recipient's ISP, where it remains until the recipient retrieves it onto his or her own computer. Every computer on the Internet has a unique numerical address (an Internet Protocol or IP address), which is associated with a more readily recognizable domain name (such as "mysite.com"). As the e-mail message travels from sender to recipient, each computer transmitting the message attaches identifying data to the "Received" field in the header. The information serves as a kind of electronic postmark for the handling of the message. It is possible for a sender to alter (or "spoof") the header information by misidentifying either the computer from which the message originated or other computers along the transmission path.

In 2003, Congress passed the Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 (CAN-SPAM), now codified at 15 U.S.C. §§ 7701 *et seq*. It prohibits the use of false or misleading header information in commercial emails, and requires all businesses to offer recipients the ability to opt out of receiving future messages. (We will not study the details further in this course, but you can find an overview at the FTC's web site.) It also includes a preemption provision, which reads, in part:

> (b) State law
>
> (1) In general
>
> This chapter supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto.
>
> (2) State law not specific to electronic mail
>
> This chapter shall not be construed to preempt the applicability of—
>
> (A) State laws that are not specific to electronic mail, including State trespass, contract, or tort law; or
>
> (B) other State laws to the extent that those laws relate to acts of fraud or computer crime.

3) Which provisions, if any, of DASA are still enforceable after the effective date of CAN-SPAM?

4) Should spam be regulated at the state level? Federally? Internationally? Not at all?

CLASS 6: INTERMEDIARIES

Today, we introduce our third major theme: the power of Internet intermediaries. We've already seen the role that ISPs play in making Internet content accessible. That gives the government power—control what the ISPs do and you control what users see. But it also gives the ISPs themselves power. And they're not alone. Web hosts like YouTube can choose what videos are available; search engines like Google can choose which sites users are directed to. Intermediaries can even choose which email gets through and which doesn't.

This raises another fundamental question of Internet law and policy: who should decide how intermediaries use this power? Should they be free to exercise it as they wish, answerable only to their customers and their shareholders? Should they be required to follow specific governmental polices? Or something in between—both a zone of discretion and limits to that discretion? If so, where do we put the line, and who decides when it has been crossed?

We start with *Marsh v. Alabama*, a classic Supreme Court case about company towns. It stands—or perhaps stood—for the principle that at some point, a private corporation can take on so many governmental regulations that it will be held to the same free speech obligations as a government would be. Courts have steadfastly refused to apply it online, and today's problems will lead us to ask why, and whether this is a correct decision.

Jumping ahead to modern issues, today's long reading is an article about Google, the biggest fish presently in the pond. The *SearchKing* case was the first in a string of failed lawsuits against search engines by web sites upset over their ranking. And the two problems will introduce us to online videogaming and provide another perspective on the spam problem. All of them raise the same question: when an intermediary should be held accountable and when it should be given free rein.

Preparation questions:

(1) What facts about Chickasaw made the Supreme Court willing to treat its streets as public, rather than private? What values was the Court trying to protect? Keep these questions in mind as you proceed.

(2) The first interesting thing in the Rosen article about Google—which provides a transition from last time into this class—is how Nicole Wong's team at Google affects the debates over governmental regulation. How does she push back against governmental attempts to control the Internet? How does she facilitate them? How does she help create a bordered Internet?

(3) The second interesting thing in the Rosen article is the fact that Nicole Wong is a private employee at a private company, but she decides whether Google users are permitted to see Ataturk's head on Carson Kressley's body. What else does she get to decide? Do you want her to stand up to or give in to Joe Lieberman? Michelle Malkin? Shiv Sena? Are her principles the same as yours? How did she get the right to impose her values on the world? (Or is there something unfair about that last question? If so, what?)

(4) The third interesting thing in the Rosen article is that Google has a *lot* of these judgment calls to make. Nicole Wong is trying to be consistent across multiple cases, and Google has plenty of other people also trying to be effective and consistent. That makes this an administrative problem. Is she, as Rosen asks, a judge? An editor? An enabler, as she

describes herself? Or something else? Would you change the *process* by which she and the other Googlers make their decisions?

(5) Why might Google have lowered Search King's ranking? SearchKing has its suspicions, but are there any potentially legitimate reasons? What do you as a user want when you use Google? How does your answer affect the analysis of whether a search result is "objective" or "subjective?" How does it affect the question of who ought to win this case?

(6) Obviously, all of today's readings deal with when a private Internet company must answer for its decisions. But a related running theme is is the question of transparency. When must the company explain what it's doing? How does transparency necessary to oversight? Could transparency be sufficient by itself—i.e., perhaps Google can rank sites however it wants, but must disclose the algorithms it uses to create the rankings? Are there any downsides to transparency?

(7) What do you think of the proposed Global Online Freedom Act described in the Rosen article? Is it a good idea or a bad one? Should the United States prohibit United States-based companies from selling Internet filtering equipment to the Chinese government? From revealing the names of dissidents to the Chinese government?

(8) One last time. In light of the role of intermediaries, has governmental power increased or decreased in the Internet age?

Marsh v. Alabama
326 U.S. 501 (1946)

MR. JUSTICE BLACK delivered the opinion of the Court.

In this case we are asked to decide whether a State, consistently with the *First* and *Fourteenth Amendments*, can impose criminal punishment on a person who undertakes to distribute religious literature on the premises of a company-owned town contrary to the wishes of the town's management. The town, a suburb of Mobile, Alabama, known as Chickasaw, is owned by the Gulf Shipbuilding Corporation. Except for that it has all the characteristics of any other American town. The property consists of residential buildings, streets, a system of sewers, a sewage disposal plant and a "business block" on which business places are situated. A deputy of the Mobile County Sheriff, paid by the company, serves as the town's policeman. Merchants and service establishments have rented the stores and business places on the business block and the United States uses one of the places as a post office from which six carriers deliver mail to the people of Chickasaw and the adjacent area. The town and the surrounding neighborhood, which can not be distinguished from the Gulf property by anyone not familiar with the property lines, are thickly settled, and according to all indications the residents use the business block as their regular shopping center. To do so, they now, as they have for many years, make use of a company-owned paved street and sidewalk located alongside the store fronts in order to enter and leave the stores and the post office. Intersecting company-owned roads at each end of the business block lead into a four-lane public highway which runs parallel to the business block at a distance of thirty feet. There is nothing to stop highway traffic from coming onto the business block and upon arrival a traveler may make free use of the facilities available there. In short the town and its shopping district are accessible to and freely used by the public in general and there

is nothing to distinguish them from any other town and shopping center except the fact that the title to the property belongs to a private corporation.

Appellant, a Jehovah's Witness, came onto the sidewalk we have just described, stood near the post office and undertook to distribute religious literature. In the stores the corporation had posted a notice which read as follows: "This Is Private Property, and Without Written Permission, No Street, or House Vendor, Agent or Solicitation of Any Kind Will Be Permitted." Appellant was warned that she could not distribute the literature without a permit and told that no permit would be issued to her. She protested that the company rule could not be constitutionally applied so as to prohibit her from distributing religious writings. When she was asked to leave the sidewalk and Chickasaw she declined. The deputy sheriff arrested her and she was charged in the state court with violating Title 14, § 426 of the 1940 Alabama Code which makes it a crime to enter or remain on the premises of another after having been warned not to do so. Appellant contended that to construe the state statute as applicable to her activities would abridge her right to freedom of press and religion contrary to the *First* and *Fourteenth Amendments to the Constitution*. This contention was rejected and she was convicted. The Alabama Court of Appeals affirmed the conviction, holding that the statute as applied was constitutional because the title to the sidewalk was in the corporation and because the public use of the sidewalk had not been such as to give rise to a presumption under Alabama law of its irrevocable dedication to the public. 21 So. 2d 558. The State Supreme Court denied certiorari, 246 Ala. 539, 21 So. 2d 564, and the case is here on appeal under § 237 (a) of the Judicial Code, 28 U. S. C. § 344 (a).

Had the title to Chickasaw belonged not to a private but to a municipal corporation and had appellant been arrested for violating a municipal ordinance rather than a ruling by those appointed by the corporation to manage a company town it would have been clear that appellant's conviction must be reversed. Under our decision in *Lovell v. Griffin*, 303 U.S. 444 and others which have followed that case, neither a State nor a municipality can completely bar the distribution of literature containing religious or political ideas on its streets, sidewalks and public places or make the right to distribute dependent on a flat license tax or permit to be issued by an official who could deny it at will. We have also held that an ordinance completely prohibiting the dissemination of ideas on the city streets cannot be justified on the ground that the municipality holds legal title to them. *Jamison v. Texas*, 318 U.S. 413. And we have recognized that the preservation of a free society is so far dependent upon the right of each individual citizen to receive such literature as he himself might desire that a municipality could not, without jeopardizing that vital individual freedom, prohibit door to door distribution of literature. *Martin v. Struthers*, 319 U.S. 141, 146, 147. From these decisions it is clear that had the people of Chickasaw owned all the homes, and all the stores, and all the streets, and all the sidewalks, all those owners together could not have set up a municipal government with sufficient power to pass an ordinance completely barring the distribution of religious literature. Our question then narrows down to this: Can those people who live in or come to Chickasaw be denied freedom of press and religion simply because a single company has legal title to all the town? For it is the State's contention that the mere fact that all the property interests in the town are held by a single company is enough to give that company power, enforceable by a state statute, to abridge these freedoms.

We do not agree that the corporation's property interests settle the question. The State urges in effect that the corporation's right to control the inhabitants of Chickasaw is coextensive with the right of a homeowner to regulate the conduct of his guests. We cannot accept that

contention. Ownership does not always mean absolute dominion. The more an owner, for his advantage, opens up his property for use by the public in general, the more do his rights become circumscribed by the statutory and constitutional rights of those who use it. *Cf. Republic Aviation Corp. v. Labor Board*, 324 U.S. 793, 798, 802, n. 8. Thus, the owners of privately held bridges, ferries, turnpikes and railroads may not operate them as freely as a farmer does his farm. Since these facilities are built and operated primarily to benefit the public and since their operation is essentially a public function, it is subject to state regulation. . . .

We do not think it makes any significant constitutional difference as to the relationship between the rights of the owner and those of the public that here the State, instead of permitting the corporation to operate a highway, permitted it to use its property as a town, operate a "business block" in the town and a street and sidewalk on that business block. *Cf. Barney v. Keokuk, 94 U.S. 324, 340*. Whether a corporation or a municipality owns or possesses the town the public in either case has an identical interest in the functioning of the community in such manner that the channels of communication remain free. As we have heretofore stated, the town of Chickasaw does not function differently from any other town. The "business block" serves as the community shopping center and is freely accessible and open to the people in the area and those passing through. The managers appointed by the corporation cannot curtail the liberty of press and religion of these people consistently with the purposes of the Constitutional guarantees, and a state statute, as the one here involved, which enforces such action by criminally punishing those who attempt to distribute religious literature clearly violates the *First* and *Fourteenth Amendments to the Constitution*. . . .

Jeffrey Rosen, *Google's Gatekeepers*
N. Y. TIMES (November 30, 2008)

In March of last year, Nicole Wong, the deputy general counsel of Google, was notified that there had been a precipitous drop in activity on YouTube in Turkey, and that the press was reporting that the Turkish government was blocking access to YouTube for virtually all Turkish Internet users. Apparently unaware that Google owns YouTube, Turkish officials didn't tell Google about the situation: a Turkish judge had ordered the nation's telecom providers to block access to the site in response to videos that insulted the founder of modern Turkey, Mustafa Kemal Ataturk, which is a crime under Turkish law. Wong scrambled to figure out which videos provoked the court order and made the first in a series of tense telephone calls to Google's counsel in London and Turkey, as angry protesters gathered in Istanbul. Eventually, Wong and several colleagues concluded that the video that sparked the controversy was a parody news broadcast that declared, "Today's news: Kamal Ataturk was gay!" The clip was posted by Greek football fans looking to taunt their Turkish rivals.

Wong and her colleagues asked the Turkish authorities to reconsider their decision, pointing out that the original offending video had already been voluntarily removed by YouTube users. But after the video was taken down, Turkish prosecutors objected to dozens of other YouTube videos that they claimed insulted either Ataturk or "Turkishness." These clips ranged from Kurdish-militia recruitment videos and Kurdish morality plays to additional videos speculating about the sexual orientation of Ataturk, including one superimposing his image on characters

from "Queer Eye for the Straight Guy." "I remember one night, I was looking at 67 different Turkish videos at home," Wong told me recently.

After having many of the videos translated into English, Wong and her colleagues set out to determine which ones were, in fact, illegal in Turkey; which violated YouTube's terms of service prohibiting hate speech but allowing political speech; and which constituted expression that Google and YouTube would try to protect. There was a vigorous internal debate among Wong and her colleagues at the top of Google's legal pyramid. Andrew McLaughlin, Google's director of global public policy, took an aggressive civil-libertarian position, arguing that the company should protect as much speech as possible. Kent Walker, Google's general counsel, took a more pragmatic approach, expressing concern for the safety of the dozen or so employees at Google's Turkish office. The responsibility for balancing these and other competing concerns about the controversial content fell to Wong, whose colleagues jokingly call her "the Decider," after George W. Bush's folksy self-description.

Wong decided that Google, by using a technique called I.P. blocking, would prevent access to videos that clearly violated Turkish law, but only in Turkey. For a time, her solution seemed to satisfy the Turkish judges, who restored YouTube access. But last June, as part of a campaign against threats to symbols of Turkish secularism, a Turkish prosecutor made a sweeping demand: that Google block access to the offending videos throughout the world, to protect the rights and sensitivities of Turks living outside the country. Google refused, arguing that one nation's government shouldn't be able to set the limits of speech for Internet users worldwide. Unmoved, the Turkish government today continues to block access to YouTube in Turkey.

THE ONGOING DISPUTE between Google and Turkey reminds us that, throughout history, the development of new media technologies has always altered the way we think about threats to free speech. At the beginning of the 20th century, civil libertarians in America worried most about the danger of the government silencing political speech: think of Eugene V. Debs, the Socialist candidate for President, who was imprisoned in 1919 for publicly protesting American involvement during World War I. But by the late 1960s, after the Supreme Court started to protect unpopular speakers more consistently, some critics worried that free speech in America was threatened less by government suppression than by editorial decisions made by the handful of private mass-media corporations like NBC and CBS that disproportionately controlled public discourse. One legal scholar, Jerome Barron, even argued at the time that the courts should give unorthodox speakers a mandatory right of access to media outlets controlled by giant corporations.

Today the Web might seem like a free-speech panacea: it has given anyone with Internet access the potential to reach a global audience. But though technology enthusiasts often celebrate the raucous explosion of Web speech, there is less focus on how the Internet is actually regulated, and by whom. As more and more speech migrates online, to blogs and social-networking sites and the like, the ultimate power to decide who has an opportunity to be heard, and what we may say, lies increasingly with Internet service providers, search engines and other Internet companies like Google, Yahoo, AOL, Facebook and even eBay.

The most powerful and protean of these Internet gatekeepers is, of course, Google. With control of 63 percent of the world's Internet searches, as well as ownership of YouTube, Google has enormous influence over who can find an audience on the Web around the world. As an acknowledgment of its power, Google has given Nicole Wong a central role in the company's

decision-making process about what controversial user-generated content goes down or stays up on YouTube and other applications owned by Google, including Blogger, the blog site; Picasa, the photo-sharing site; and Orkut, the social networking site. Wong and her colleagues also oversee Google's search engine: they decide what controversial material does and doesn't appear on the local search engines that Google maintains in many countries in the world, as well as on Google.com. As a result, Wong and her colleagues arguably have more influence over the contours of online expression than anyone else on the planet.

In response to the rise of online gatekeepers like Wong, some House Democrats and Republicans have introduced a bipartisan bill called the Global Online Freedom Act, which would require that Internet companies disclose to a newly created office in the State Department all material filtered in response to demands by foreign governments. Google and other leading Internet companies have sought modifications to the bill, arguing that, without the flexibility to negotiate (as Wong did with Turkey), they can't protect the safety of local employees and that they may get kicked out of repressive countries, where they believe even a restricted version of their services does more good than harm. For the past two years, Google, Yahoo and Microsoft, along with other international Internet companies, have been meeting regularly with human rights and civil-liberties advocacy groups to agree on voluntary standards for resisting worldwide censorship requests. At the end of last month, the Internet companies and the advocacy groups announced the Global Network Initiative, a series of principles for protecting global free expression and privacy.

Voluntary self-regulation means that, for the foreseeable future, Wong and her colleagues will continue to exercise extraordinary power over global speech online. Which raises a perennial but increasingly urgent question: Can we trust a corporation to be good — even a corporation whose informal motto is "Don't be evil"?

"To love Google, you have to be a little bit of a monarchist, you have to have faith in the way people traditionally felt about the king," Tim Wu, a Columbia law professor and a former scholar in residence at Google, told me recently. "One reason they're good at the moment is they live and die on trust, and as soon as you lose trust in Google, it's over for them." Google's claim on our trust is a fragile thing. After all, it's hard to be a company whose mission is to give people all the information they want and to insist at the same time on deciding what information they get.

THE HEADQUARTERS OF YOUTUBE are in a former Gap building in San Bruno, Calif., just a few miles from the San Francisco International Airport. In the lobby, looming over massage chairs, giant plasma-screen TVs show popular videos and scroll news stories related to YouTube. The day I arrived to interview the YouTube management about how the site regulates controversial speech, most of the headlines, as it happens, had to do with precisely that topic. Two teenagers who posted a video of themselves throwing a soft drink at a Taco Bell employee were ordered by a Florida judge to post an apology on YouTube. The British culture secretary had just called on YouTube to carry warnings on clips that contain foul language.

The volume of videos posted on YouTube is formidable — Google estimates that something like 13 hours of content are uploaded every minute. YouTube users can flag a video if they think it violates YouTube's community guidelines, which prohibit sexually explicit videos, graphic violence and hate speech. Once flagged, a video is vetted by YouTube's internal reviewers at facilities around the world who decide whether to take it down, leave it up or send it up the

YouTube hierarchy for more specialized review. When I spoke with Micah Schaffer, a YouTube policy analyst, he refused to say how many reviewers the company employs. But I was allowed to walk around the office to see if I could spot any of them. I passed one 20-something YouTube employee after another — all sitting in cubicles and wearing the same unofficial uniform of T-shirt and jeans. The internal reviewers were identifiable, I was told, only by the snippets of porn flickering on their laptops.

The idea of a 20-something with a laptop in San Bruno (or anywhere else, for that matter) interpreting community guidelines for tens of millions of users might not instill faith in YouTube's vetting process. But the most controversial user flags or requests from foreign governments make their way up the chain of command to the headquarters of Google, in Mountain View, Calif., where they may ultimately be reviewed by Wong, McLaughlin and Walker.

Recently, I spent several days talking to Wong and her colleagues at the so-called Googleplex, which has the feeling of a bucolic and extraordinarily well-financed theme camp. As we sat around a conference table, they told me about their debates as they wrestled with hard cases like the dispute in Turkey, as well as the experiences that have informed their thinking about free speech. Walker, the general counsel, wrote for The Harvard Crimson as an undergraduate and considered becoming a journalist before going into law; McLaughlin, the head of global public policy, became a fellow at Harvard's Berkman Center for Internet and Society after working on the successful Supreme Court challenge to part of the federal Communications Decency Act. And Wong, a soft-spoken and extremely well organized woman, has a joint degree in law and journalism from Berkeley and told me she aspired to be a journalist as a child because of her aunt, a reporter for The Los Angeles Times.

I asked Wong what was the best analogy for her role at Google. Was she acting like a judge? An editor? "I don't think it's either of those," she said. "I definitely am not trying to pass judgment on anything. I'm taking my best guess at what will allow our products to move forward in a country, and that's not a judge role, more an enabling role." She stressed the importance for Google of bringing its own open culture to foreign countries while still taking into account local laws, customs and attitudes. "What is the mandate? It's 'Be everywhere, get arrested nowhere and thrive in as many places as possible.' " So far, no Google employees have been arrested on Wong's watch, though some have been detained.

When Google was founded, 10 years ago, it wasn't at all obvious whether the proprietors of search engines would obey the local laws of the countries in which they did business — and whether they would remove links from search results in response to requests from foreign governments. This began to change in 2000, when a French Jew surfed a Yahoo auction site to look for collections of Nazi memorabilia, which violated a French law banning the sale and display of anything that incites racism. After a French judge determined that it was feasible for Yahoo to identify 90 percent of its French users by analyzing their I.P. addresses and to screen the material from the users, he ordered Yahoo to make reasonable efforts to block French users from accessing the prohibited content or else to face fines and the seizure of income from Yahoo's French subsidiary. In January 2001, Yahoo banned the sale of Nazi memorabilia on its Web sites.

The Yahoo case was a landmark. It made clear that search engines like Google and Yahoo could be held liable outside the United States for indexing or directing users to content after having been notified that it was illegal in a foreign country. In the United States, by contrast,

Internet service providers are protected from most lawsuits involving having hosted or linked to illegal user-generated content. As a consequence of these differing standards, Google has considerably less flexibility overseas than it does in the United States about content on its sites, and its "information must be free" ethos is being tested abroad.

For example, on the German and French default Google search engines, Google.de and Google.fr, you can't find Holocaust-denial sites that can be found on Google.com, because Holocaust denial is illegal in Germany and France. In the wake of the Yahoo decision, Google decided to comply with governmental requests to take down links on its national search engines to material that clearly violates national laws. (In the interest of disclosure, however, Google has agreed to report all the links it takes down in response to government demands to chillingeffects.com, a Web site run by Harvard's Berkman Center that keeps a record of censored online materials.)

Of course, not every overseas case presents a clear violation of national law. In 2006, for example, protesters at a Google office in India demanded the removal of content on Orkut, the social networking site, that criticized Shiv Sena, a hard-line Hindu political party popular in Mumbai. Wong eventually decided to take down an Orkut group dedicated to attacking Shivaji, revered as a deity by the Shiv Sena Party, because it violated Orkut terms of service by criticizing a religion, but she decided not to take down another group because it merely criticized a political party. "If stuff is clearly illegal, we take that down, but if it's on the edge, you might push a country a little bit," Wong told me. "Free-speech law is always built on the edge, and in each country, the question is: Can you define what the edge is?"

INITIALLY, GOOGLE'S POLICY of removing links to clearly illegal material on its foreign search engines seemed to work. But things changed significantly after Google bought and expanded YouTube in 2006. Once YouTube was available in more than 20 countries and in 14 languages, users began flagging hundreds of videos that they saw as violations of local community standards, and governments around the globe demanded that certain videos be blocked for violating their laws. Google's solution was similar to the one the French judge urged on Yahoo: it agreed to block users in a particular country from accessing videos that were clearly illegal under local law. But that policy still left complicated judgment calls in murkier cases.

In late 2006, for example, Wong and her colleagues debated what to do about a series of videos that insulted the king of Thailand, where a lêse-majesté law makes criticisms of the king a criminal offense. Wong recalls hearing from an employee in Asia that the Thai government had announced that it was blocking access to YouTube for anyone with a Thai I.P. address. Soon after, a Thai government official sent Wong a list of the U.R.L.'s of 20 offensive videos that he demanded Google remove as a condition of unblocking the site. Some of the videos were sexually explicit or involved hate speech and thus clearly violated the YouTube terms of service. Some ridiculed the king — by depicting him with his feet on his head, for example — and were clearly illegal under Thai law but not U.S. law. And others — criticizing the Thai lêse-majesté law itself — weren't illegal in Thailand but offended the government.

After an extensive debate with McLaughlin and Walker, Wong concluded that since the lêse-majesté law had broad democratic support in Thailand, it would be better to remove the videos that obviously violated Thai law while refusing to remove the videos that offended the government but didn't seem to be illegal. All three told me they were reassured by the fact that Google could accommodate the Thai government by blocking just the videos that were clearly

illegal in Thailand (and blocking those for Thai users only), leaving them free to exercise their independent judgment about videos closer to the line. The Thai government was apparently able to live with this solution.

Over the past couple of years, Google and its various applications have been blocked, to different degrees, by 24 countries. Blogger is blocked in Pakistan, for example, and Orkut in Saudi Arabia. Meanwhile, governments are increasingly pressuring telecom companies like Comcast and Verizon to block controversial speech at the network level. Europe and the U.S. recently agreed to require Internet service providers to identify and block child pornography, and in Europe there are growing demands for network-wide blocking of terrorist-incitement videos. As a result, Wong and her colleagues said they worried that Google's ability to make case-by-case decisions about what links and videos are accessible through Google's sites may be slowly circumvented, as countries are requiring the companies that give us access to the Internet to build top-down censorship into the network pipes.

IT'S NOT ONLY FOREIGN COUNTRIES that are eager to restrict speech on Google and YouTube. Last May, Senator Joseph Lieberman's staff contacted Google and demanded that the company remove from YouTube dozens of what he described as jihadist videos. (Around the same time, Google was under pressure from "Operation YouTube Smackdown," a grass-roots Web campaign by conservative bloggers and advocates to flag videos and ask YouTube to remove them.) After viewing the videos one by one, Wong and her colleagues removed some of the videos but refused to remove those that they decided didn't violate YouTube guidelines. Lieberman wasn't satisfied. In an angry follow-up letter to Eric Schmidt, the C.E.O. of Google, Lieberman demanded that all content he characterized as being "produced by Islamist terrorist organizations" be immediately removed from YouTube as a matter of corporate judgment — even videos that didn't feature hate speech or violent content or violate U.S. law. Wong and her colleagues responded by saying, "YouTube encourages free speech and defends everyone's right to express unpopular points of view." In September, Google and YouTube announced new guidelines prohibiting videos "intended to incite violence."

In addition to Lieberman, another outspoken critic of supposed liberal bias at YouTube and Google is Michelle Malkin, the conservative columnist and blogger. Malkin became something of a cause célèbre among YouTube critics in 2006, when she created a two-minute movie called "First, They Came" in the wake of the violent response to the Danish anti-Muhammad cartoons. After showing pictures of the victims of jihadist violence (like the Dutch filmmaker Theo Van Gogh) and signs declaring "Behead Those Who Insult Islam," the video asks, "Who's next?" and displays the dates of terrorist attacks in America, London, Madrid and Bali.

Nearly seven months after she posted the video, Malkin told me she was "flabbergasted" to receive an e-mail message from YouTube saying the video had been removed for its "inappropriate content." When Malkin asked why the video was removed, she received no response, and when she posted a video appealing to YouTube to reinstate it, that video, too, was deleted with what she calls the "false claim" that it had been removed at her request. Malkin remains dissatisfied with YouTube's response. "I'm completely flummoxed about what their standards are," she said. "The standards need to be clear, they need to be consistent and they need to be more responsive."

I watched the "First, They Came" video, which struck me as powerful political commentary that contains neither hate speech nor graphic violence, and I asked why it was taken down.

According to a YouTube spokesman, the takedown was a routine one that hadn't been reviewed by higher-ups. The spokesman said he couldn't comment on particular cases, but he forwarded a link to Malkin's current YouTube channel, noting that it contains 55 anti-jihadist videos similar to "First, They Came," none of which have been taken down. ("First, They Came" can now be found on Malkin's YouTube channel, too.)

The removal of Malkin's video may have been an innocent mistake. But it serves as a reminder that one person's principled political protest is another person's hate speech, and distinguishing between the two in hard cases is a lot to ask of a low-level YouTube reviewer. In addition, the publicity that attended the removal of Malkin's video only underscores the fact that in the vast majority of cases in which material is taken down, the decision to do so is never explained or contested. The video goes down, and that's the end of it.

Yet even in everyday cases, it's often no easier to determine whether the content of a video is actually objectionable. When I visited YouTube, the management showed me a flagged French video of a man doubled over. Was he coughing? Or in pain? Or playacting? It was hard to say. The YouTube managers said they might send the item to a team of French-language reviewers for further inspection, but if the team decided to take down the video, its reasons would most likely never become public.

AS THE LAW PROFESSOR TIM WU TOLD ME, to trust Google, you have to be something of a monarchist, willing to trust the near-sovereign discretion of Wong and her colleagues. That's especially true in light of the Global Network Initiative, the set of voluntary principles for protecting free expression and privacy endorsed last month by leading Internet companies like Google and leading human rights and online-advocacy groups like the Center for Democracy and Technology. Google and other companies say they hope that by acting collectively, they can be more effective in resisting censorship requests from repressive governments and, when that isn't possible, create a trail of accountability.

Google is indeed more friendly to free speech than the governments of most of the countries in which it operates. But even many of those who are impressed by Wong and her colleagues say the Google "Decider" model is impractical in the long run, because, as broadband use expands rapidly, it will be unrealistic to expect such a small group of people to make ad hoc decisions about permissible speech for the entire world. "It's a 24-hour potential problem, every moment of the day, and because of what the foreign governments can do, like put people in jail, it creates a series of issues that are very, very difficult to deal with," Ambassador David Gross, the U.S. coordinator for International Communications and Information Policy at the State Department, told me. I asked Wong whether she thought the Decider model was feasible in the long term, and to my surprise, she said no. "I think the Decider model is an inconsistent model because the Internet is big and Google isn't the only one making the decisions," she told me.

When I pressed Wong and her colleagues about who they thought should make these decisions, they said they would be happiest, of course, if more countries would adopt U.S.-style free-speech protections. Knowing that that is unlikely, they said they would prefer that countries around the world set up accountable bodies that provide direct guidance about what controversial content to restrict. As an example of his preferred alternative, Andrew McLaughlin pointed to Germany, which has established a state agency that gathers the U.R.L.'s of sites hosting Nazi and violent content illegal under German law and gives the list to an industry body, which then passes it on to Google so that it can block the material on its German site. (Whenever

Google blocks material there or on its other foreign sites, it indicates in the search results that it has done so.)

It is striking — and revealing — that Wong and her colleagues would prefer to put themselves out of business. But it is worth noting that even if Google's suggestion were adopted, and governments around the world began to set up national review boards that told Google what content to remove, then those review boards might protect far less free speech than Google's lawyers have. When I raised this concern, McLaughlin said he hoped that the growing trends to censor speech, at the network level and elsewhere, would be resisted by millions of individual users who would agitate against censorship as they experienced the benefits of free speech.

There's much to be said for McLaughlin's optimism about online free-speech activism. Consider recent experiences in Turkey, where a grass-roots "censuring the censors" movement led more than 400 Turkish bloggers to shutter their Web sites in solidarity with mainstream sites that were banned for carrying content that, among other things, insulted Turkey's founding father. In America, and around the world, the boundaries of free speech have always been shaped more by political activism than by judicial decisions or laws. But what is left out of McLaughlin's vision is uncertainty about one question: the future ethics and behavior of gatekeepers like Google itself.

"Right now, we're trusting Google because it's good, but of course, we run the risk that the day will come when Google goes bad," Wu told me. In his view, that day might come when Google allowed its automated Web crawlers, or search bots, to be used for law-enforcement and national-security purposes. "Under pressure to fight terrorism or to pacify repressive governments, Google could track everything we've searched for, everything we're writing on gmail, everything we're writing on Google docs, to figure out who we are and what we do," he said. "It would make the Internet a much scarier place for free expression." The question of free speech online isn't just about what a company like Google lets us read or see; it's also about what it does with what we write, search and view.

WU'S FEARS THAT violations of privacy could chill free speech are grounded in recent history: in China in 2004, Yahoo turned over to the Chinese government important account information connected to the e-mail address of Shi Tao, a Chinese dissident who was imprisoned as a result. Yahoo has since come to realize that the best way of resisting subpoenas from repressive governments is to ensure that private data can't be turned over, even if a government demands it. In some countries, I was told by Michael Samway, who heads Yahoo's human rights efforts, Yahoo is now able to store communications data and search queries offshore and limits access of local employees, so Yahoo can't be forced to turn over this information even if it is ordered to do so.

Isolating, or better still, purging data is the best way of protecting privacy and free expression in the Internet age: it's the only way of guaranteeing that government officials can't force companies like Google and Yahoo to turn over information that allows individuals to be identified. Google, which refused to discuss its data-purging policies on the record, has raised the suspicion of advocacy groups like Privacy International. Google announced in September that it would anonymize all the I.P. addresses on its server logs after nine months. Until that time, however, it will continue to store a wealth of personal information about our search results and viewing habits — in part to improve its targeted advertising and therefore its profits. As Wu

suggests, it would be a catastrophe for privacy and free speech if this information fell into the wrong hands.

"The idea that the user is sovereign has transformed the meaning of free speech," Wu said enthusiastically about the Internet age. But Google is not just a neutral platform for sovereign users; it is also a company in the advertising and media business. In the future, Wu said, it might slant its search results to favor its own media applications or to bury its competitors. If Google allowed its search results to be biased for economic reasons, it would transform the way we think about Google as a neutral free-speech tool. The only editor is supposed to be a neutral algorithm. But that would make it all the more insidious if the search algorithm were to become biased.

"During the heyday of Microsoft, people feared that the owners of the operating systems could leverage their monopolies to protect their own products against competitors," says the Internet scholar Lawrence Lessig of Stanford Law School. "That dynamic is tiny compared to what people fear about Google. They have enormous control over a platform of all the world's data, and everything they do is designed to improve their control of the underlying data. If your whole game is to increase market share, it's hard to do good, and to gather data in ways that don't raise privacy concerns or that might help repressive governments to block controversial content."

Given their clashing and sometimes self-contradictory missions — to obey local laws, repressive or not, and to ensure that information knows no bounds; to do no evil and to be everywhere in a sometimes evil world — Wong and her colleagues at Google seem to be working impressively to put the company's long-term commitment to free expression above its short-term financial interests. But they won't be at Google forever, and if history is any guide, they may eventually be replaced with lawyers who are more concerned about corporate profits than about free expression. "We're at the dawn of a new technology," Walker told me, referring not simply to Google but also to the many different ways we now interact online. "And when people try to come up with the best metaphors to describe it, all the metaphors run out. We've built this spaceship, but we really don't know where it will take us."

Search King, Inc. v. Google Technologies., Inc.
2003 U.S. Dist. LEXIS 27193 (W.D. Okla. May 27, 2003)

This matter is before the Court on Defendant Google Technology, Inc.'s ("Google") Motion to Dismiss Plaintiff Search King, Inc.'s ("Search King") Complaint pursuant to *Federal Rule of Civil Procedure 12(b)(6)*. The matter has been fully briefed and is now ripe for determination. Upon review of the parties' submissions, and for the reasons set forth below, the Court grants Google's motion to dismiss.

I. Introduction

This case involves the interrelationship between Internet search engines and Internet advertising, and their collective connection to the *First Amendment*. More specifically, the questions at issue are whether a representation of the relative significance of a web site as it corresponds to a search query is a form of protected speech, and if so, whether the "speaker" is therefore insulated from tort liability arising out of the intentional manipulation of such a representation under Oklahoma law.

Google operates an Internet search engine.[1] Every search engine is controlled by a mathematical algorithm. One component of Google's mathematical algorithm produces a "PageRank," which is a numerical representation of the relative significance of a particular web site as it corresponds to a search query. The PageRank is derived from a combination of factors that include text-matching and the number of links from other web sites that point to the PageRanked web site.[2] The higher the PageRank,[3] the more closely the web site in question ostensibly matches the search query, and vice versa. Google does not sell PageRanks, and the web sites that arc ranked have no power to determine where they are ranked, or indeed whether they are included on Google's search engine at all.

1 Search engines are indexing tools used to locate web sites that correspond to a user's search query. Search queries typically consist of one or more words or phrases that identify or are related to the subject of the search.

2 Although PageRanks are not displayed on Google's web site, they can be observed via a free "toolbar" that may be downloaded from Google's web site.

3 PageRank values range between 1 and 10.

Notwithstanding the fact that PageRanks cannot be purchased, they do have value. For example, highly-ranked web sites can charge a premium for advertising space. PR Ad Network ("PRAN," and together with Search King, "Search King"), which was introduced by Search King in August of 2002, capitalizes on this benefit by acting as a middleman, charging its clients a fee for locating highly-ranked web sites receptive to the idea of advertising on their sites, and in turn compensating those highly-ranked web sites with a portion of its fee. PRAN's fee is based, in part, on the PageRank assigned to the web site on which its client's advertisement and/or link is placed.

This action is based upon a PageRank reduction. From approximately February of 2001 until July of 2002, Search King's PageRank was 7. In July of 2002, Search King's PageRank was increased to 8. Before it was decreased, PRAN's PageRank was 2. In August or September of 2002, Search King's PageRank dropped to 4; PRAN's PageRank was eliminated completely, resulting in "no rank." The devaluation is alleged to have adversely impacted the business opportunities available to Search King and PRAN to an indeterminate degree by limiting their exposure on Google's search engine.

Shortly after the PageRank decreases, Search King filed the instant action alleging tortious interference with contractual relations and seeking injunctive relief,[4] compensatory and punitive damages. Specifically, Search King alleges Google purposefully and maliciously decreased the PageRanks previously assigned to Search King, PRAN, and certain unidentified, affiliated web sites on Google's Internet search engine in August or September of 2002. Search King asserts the devaluation occurred after and because Google learned that PRAN was competing with Google and that it was profiting by selling advertising space on web sites ranked highly by Google's PageRank system. Google asserts it is immune from tort liability arising out of the devaluation because PageRanks constitute protected speech.

4 Search King's motion for a preliminary injunction was denied by previous order of this Court.

II. Discussion

Motions to dismiss a complaint for failure to state a claim should be granted only where "no relief could be granted under any set of facts that could be proved consistent with the allegations." *Swierkiewicz v. Sorema N.A.*, 534 U.S. 506, 514, 122 S. Ct. 992, 152 L. Ed. 2d 1 (2002) (quoting *Hishon v. King & Spalding*, 467 U.S. 69, 73, 104 S. Ct. 2229, 81 L. Ed. 2d 59 (1984)). When considering a motion filed pursuant to *Rule 12(b)(6)*, "[a]ll well-pleaded factual allegations in the complaint are accepted as true ... and viewed in the light most favorable to the nonmoving party ...." *GFF Corp. v. Associated Wholesale Grocers, Inc.*, 130 F.3d 1381, 1384 (10th Cir. 1997) (internal citations omitted). "The issue in reviewing the sufficiency of a complaint is not whether the plaintiff will prevail, but whether the plaintiff is entitled to offer evidence to support [its] claims." *Ruiz v. McDonnell*, 299 F.3d 1173, 1181 (10th Cir. 2002).

Search King asserts a single cause of action — tortious interference with contractual relations.[5] Under Oklahoma law, such an action requires a plaintiff to demonstrate: (1) the defendant interfered with a business or contractual relationship of the plaintiff; (2) the interference was malicious and wrongful, and was not justified, privileged, or excusable; and (3) the plaintiff suffered injury as a proximate result of the interference. *See Daniels v. Union Baptist Ass'n*, 2001 OK 63, 55 P.3d 1012, 1015 (Okla. 2001). The parties concede that this case turns on the second factor.[6] The Court must, therefore, determine whether Google's manual decrease of Search King's PageRank was malicious and wrongful, and was not justified, privileged, or excusable. Google asserts that its actions cannot be considered wrongful because PageRanks constitute opinions protected by the *First Amendment*. In support of that proposition, Google relies on *Jefferson County Sch. Dist. No. R-1 v. Moody's Investor's Services, Inc.*, 175 F.3d 848 (10th Cir. 1999).

5 In its Amended Complaint, Search King identifies two "causes of action." However, the first simply consists of a request for injunctive relief and, as such, does not constitute a separate cause of action.

6 The Court will assume, *arguendo*, that one or more of Search King's contractual relationships was adversely affected by the PageRank decreases and that Search King was injured as a proximate result of those decreases.

In *Jefferson County*, the Tenth Circuit, relying on the Supreme Court's holding that "a statement of opinion relating to matters of public concern which does not contain a provably false factual connotation will receive full constitutional protection," *Jefferson County*, 175 F.3d at 852 (quoting *Milkovich v. Lorain Journal Co.*, 497 U.S. 1, 20, 110 S. Ct. 2695, 111 L. Ed. 2d 1 (1990)), held that *First Amendment* protection extended to a financial rating service's unfavorable review of the value of a school district's refunding bonds. *See id.* at 852-55. At the same time, the court dispensed with the school district's allegation that Moody's acted intentionally and with malice, noting that "even when a speaker or writer is motivated by hatred or illwill his expression [is] protected by the *First Amendment*." *Id.* at 857-58 (quoting *Hustler Magazine v. Falwell*, 485 U.S. 46, 53, 108 S. Ct. 876, 99 L. Ed. 2d 41 (1988) (alteration in original)). Based in large part on the constitutional protection afforded the review, the Tenth Circuit affirmed the district court order granting Moody's motion to dismiss the school district's claims for intentional interference with contract, intentional interference with business relations, and publication of an injurious falsehood. *See id.* at 860.

Search King contends that PageRanks are objectively verifiable, and that *Jefferson County* is therefore distinguishable from the instant case. First, Search King notes that Lawrence Page ("Page"), the founder of Google and the inventor of the PageRank system, holds a U.S. patent on

the system. Search King argues that because ideas are not patentable, *see Gottschalk v. Benson*, 409 U.S. 63, 67, 93 S. Ct. 253, 34 L. Ed. 2d 273 (1972), and because patented products or processes must be replicable, *see* 37 C.F.R. § 1.71(a) (2003) (providing that a patent specification must "include a written description of the invention or discovery and of the manner and process of making and using the same, and is required to be in such full, clear, concise, and exact terms as to enable any person skilled in the art or science to which the invention or discovery appertains, or with which it is most nearly connected, to make and use the same"), the PageRank system must be objective in nature, and therefore capable of being proven true or false.

Next, Search King points out that in his doctoral thesis at Stanford University, Page describes the PageRank system as objective and mechanical, and also notes that Google's web site declares the PageRank system "honest and objective." Search King argues that Google cannot "have it both ways," professing the objectivity of the PageRank system on one hand, and relying on the subjective nature of the system in order to avoid tort liability on the other.

Two questions remain. First, are PageRanks constitutionally protected opinions? Second, if PageRanks fall within the scope of protection afforded by the *First Amendment*, is the publication of PageRanks *per se* lawful under Oklahoma law, thereby precluding tort liability premised on the intentional and even malicious manipulation of PageRanks by Google? The Court answers both questions in the affirmative.

"It is always a question for the court to determine as a matter of law whether a published statement is within the protected class of speech." *Gaylord Entertainment Co. v. Thompson*, 1998 OK 30, 958 P.2d 128, 142 (Okla. 1998). Google argues that PageRanks are subjective opinions, not unlike Moody's review of the school district's refunding bonds in *Jefferson County*. Search King's first argument to the contrary, with respect to the requirement that patented processes be replicable, is not wholly without merit. Because patented processes must be capable of replication, it stands to reason that the intentional deviation from such a process would result in a provably false result to the extent the result would have been different in the absence of manipulation. However, this reasoning ignores the important distinction between process and result. Here, the process, which involves the application of the PageRank algorithm, is objective in nature. In contrast, the result, which is the PageRank — or the numerical representation of relative significance of a particular web site — is fundamentally subjective in nature. This is so because every algorithm employed by every search engine is different, and will produce a different representation of the relative significance of a particular web site depending on the various factors, and the weight of the factors, used to determine whether a web site corresponds to a search query. In the case at bar, it is the subjective result, the PageRank, which was modified, and which forms the basis for Search King's tort action.

The Court finds Search King's alternative argument, with respect to certain statements regarding the purported objectivity of the PageRank system, is similarly unpersuasive. As discussed above, the objective nature of the PageRank algorithm, assuming it is adhered to by Google, is not in question. But neither is it at issue. At issue is the subjective result produced by an algorithm unique to Google. Just as the alchemist cannot transmute lead into gold, Google and Page's statements as to the purported objectivity of the PageRank system cannot transform a subjective representation into an objectively verifiable fact.

In view of the foregoing discussion, the Court concludes that *Jefferson County* is analogous to the case at bar. Like the review in *Jefferson County*, the Court finds that PageRanks relate to matters

of public concern, in this case, via the "World Wide Web." In addition, the Court finds that PageRanks do not contain provably false connotations. PageRanks are opinions — opinions of the significance of particular web sites as they correspond to a search query. Other search engines express different opinions, as each search engine's method of determining relative significance is unique. The Court simply finds there is no conceivable way to prove that the relative significance assigned to a given web site is false. Accordingly, the Court concludes that Google's PageRanks are entitled to "full constitutional protection." *Jefferson County*, 175 F.3d at 852 (quoting *Milkovich*, 497 U.S. at 20).

Having determined that PageRanks are constitutionally protected opinions, the Court must now consider whether, under Oklahoma law, Google is immune from tort liability arising out of the intentional manipulation of PageRanks. In *Jefferson County*, the Tenth Circuit concluded that under Colorado law, protected speech cannot constitute improper interference in the context of a claim for tortious interference with contractual relations. *See id.* at 858. The Court finds that Oklahoma law compels the same conclusion in this case.

In *Gaylord*, the Oklahoma Supreme Court held that constitutionally protected speech is *per se* lawful and, therefore, cannot give rise to an action for tortious interference with advantageous business relations. *See Gaylord*, 958 P.2d at 149-50. Notwithstanding that the elements of a tortious interference with advantageous business relations claim differ from the elements of a tortious interference with contractual relations claim, the Court would note that both claims require that the interference be *unlawful*. *See id.* & nn. 96, 97. Therefore, the Court finds that under Oklahoma law, protected speech — in this case, PageRanks — cannot give rise to a claim for tortious interference with contractual relations because it cannot be considered wrongful, even if the speech is motivated by hatred or ill will. *See Jefferson County*, 175 F.3d at 857-58. Accordingly, the Court finds that Search King has failed to state a claim upon which relief may be granted.

III. Conclusion

In view of the foregoing, the Court hereby GRANTS Google's Motion to Dismiss and DISMISSES Search King's Complaint without prejudice. The Court DENIES Search King's Motion to Alter and/or Amend Judgment as moot.

Estavillo Problem

This problem is based on *Estavillo v. Sony Computer Entertainment America Inc.,* No. C-09-03007 RMW, 2009 U.S. Dist LEXIS 86821 (2009).

Erik Estavillo sued Sony Computer Entertainment America, which sells the PlayStation and operates the online PlayStation 3 Network. His *pro se* complaint alleged:

> 4. Sony Computer Entertainment America has caused pain and suffering to an already disabled plaintiff, who suffers from Obsessive-Compulsive Disorder, Panic Disoder, Major Depression, and Crohn's Disease. The pain and suffering was caused by the defendant, Sony, banning the plaintiff's account on the Playstation 3 Network, in which the plaintiff relies on to socialize with other people, since it's the only way the plaintiff can truly socialize since he also suffers from Agoraphobia. The plaintiff has convincing medical documents to prove all of his diseased conditions.

5. The ban is supposedly due to the behavior of the plaintiff when he plays the video game "Resistance: Fall of Man," which Sony owns and employs moderators for its online play. These moderators kick and ban players that they feel are deserving; though their biases to as player seems to be whatever determines the kick or ban from the Resistance game server. The need for moderators on Resistance is unnecessary since other players can both mute and/or ignore any player they wish.

6. In this first count, the plaintiff was exercising his First Amendment Right to Freedom of Speech in the game's public forum when he was banned from, not only the Resistance video game, but also banned from playing all other games online via the PlayStation Network. Sony's PlayStation 3 is the only gaming system that incorporates this type of wide-ranged ban. As where Nintendo does not ban customers at all. And Microsoft Xbox rarely bans, and only for repeated illegal offenses. ...

Sony moves to dismiss under F.R.C.P. 12(b)(6) for failure to state a claim. If Estavillo responds by relying on *Marsh v. Alabama*, how should the court rule?

MAPS Problem

The following is taken from the statement of facts in *Media3 Technologies LLC v. Mail Abuse Prevention System*, No. 00-CV-12524-MEL, 2001 U.S. Dist. LEXIS 1310 (D. Mass. Jan. 1, 2001):

Media3 is an Internet "web-hosting" company based in Pembroke, Massachusetts, that offers services in creating and maintaining websites to those who wish to conduct electronic commerce. As a "web-hosting" company, Media3 is the owner of forty-two "Class C network address blocks." Each block is capable of holding approximately 254 "Internet protocol addresses" on which websites may be placed. Media3 rents Internet protocol addresses on these Class C networks to individuals and organizations who wish to create websites. Often with Media3's help, these customers then build websites which Media3 also assists in maintaining.

Before agreeing to host a website, Media3 follows the standard industry practice of requiring its customers to sign an Acceptable Use Policy for conducting business on the Internet. This policy contains provisions which are standard in the industry, including an "anti-spam" provision.

Spam is the industry term used to describe unwanted e-mail that is often sent en masse to e-mail addresses for commercial purposes. For obvious reasons, spam is unpopular with many in the Internet community. One not so obvious, but critically important, reason why spam is unpopular is that while it is free to send it costs money to receive Media3's Acceptable Use Policy prohibits not only the transmission of spam, but also the support of spam through the development of software which could be used to hide the origin of a person sending spam.

Although Media3's Acceptable Use Policy bars websites it hosts from supporting spam in some ways, it does not prohibit its hosted websites from providing other services which appear to be used primarily by spammers. These services include the sale of lists of hundreds of thousands and even millions of e-mail addresses and computer software

programs which can "harvest" similar lists from the Internet. While the vast majority of Media3's customers do not offer such "spam support" services, a few do.

In May of 2000, the offending websites were brought to the attention of MAPS. MAPS is a non-profit Internet service provider based in California which, like other Internet service providers (such as America Online), provides Internet and e-mail access to its subscribers. While MAPS is organized like an ordinary ISP, its mission and role in the Internet community is distinct. MAPS' stated purpose is to combat spam. Its primary means for combating spam is its "Realtime Blackhole List." The blackhole list is a constantly updated list of the websites that, in MAPS' view, either send or support the sending of spam. When MAPS places a website on the blackhole list, it blocks transmission between the website and addresses in its system. MAPS has made its popular blackhole list available to other Internet service providers, sometimes for a fee. It is a popular product and approximately 40 percent of all internet addresses, including those of several Massachusetts enterprises, use MAPS' blackhole list as a spam filter.

In May of 2000, when MAPS learned that Media3 was hosting ten websites on one of its Class C networks which allegedly "supported spam," it contacted Media3 and requested that Media3; (1) terminate its hosting agreements with the contested websites; and (2) revise its Acceptable Use Policy to expressly prohibit the provision of "spam support" services such as the harvesting of e-mail addresses described above. If Media3 did not comply, MAPS informed Media3 that it would place on the blackhole list not only the ten contested websites but also any other websites that were on the same Class C network as the contested websites. This prospect was of some concern to Media3 because, as a hosting company, one of the primary services that it provides to its customers is ensuring that their websites are freely accessible and can easily access the Internet. Inclusion on MAPS' blackhole list would threaten Media3's ability to deliver good access to the Internet. After some exchange back and forth via e-mail and telephone between MAPS, in California, and Media3, in Massachusetts, Media3 refused to comply with MAPS's requests. MAPS then listed the disputed websites and any other websites on the same Class C network on the blackhole list.

Media3 alleges that MAPS' actions constitute defamation and have damaged its business by driving away customers. If Media3 moves for a preliminary injunction, how should the court rule?

CLASS 7: PERSONAL JURISDICTION

Now, we turn to a topic familiar from Civil Procedure: personal jurisdiction. As you no doubt recall, a court may not act in a case unless it has personal jurisdiction over the parties. The plaintiff is usually easy: he or she voluntarily submits to the court's jurisdiction. But the defendant typically doesn't consent. If she doesn't have much in the way of a connection to the state where the court sits, it would violate Due Process to subject him or her to the court's jurisdiction. The Supreme Court, in the famous *International Shoe* case, held that the court may only exercise jurisdiction where the defendant has sufficient "minimum contacts" with the forum state. Residence and physical presence suffice, and so do certain other kinds of activities that create connections with the forum.

You also no doubt recall that personal jurisdiction comes in two flavors: general and specific. General personal jurisdiction arises when the defendant has continuous and systematic contacts such that it is reasonable to force them to defend any action in the state's courts. Specific personal jurisdiction is narrower but has a lower threshold. If the defendant's actions in connection with the specific events giving rise to the plaintiff's cause of action are sufficiently connected with the forum, the plaintiff may sue there on that cause of action only. We will discuss only the Internet application of the specific jurisdiction tests.

In the past, I've taught some old and canonical cases of Internet jurisdiction: the *Inset* bright-line test and the *Zippo* sliding scale of interactivity. But those cases are getting long in the tooth, and the modern tests courts are using would make Judge Easterbrook much happier: they look a lot more like the traditional offline tests. Thus, I've given you two more typical cases: one a tort action (*Young*), and one a contract case (*Boschetto*). Both of them find no jurisdiction, but query whether they're correctly decided. As you should by now have figured out, some particularly important issues come up only in the problems, so be on the lookout for curveballs.

Preparation Questions:

(1) We've seen jurisdictional issues before, of course. Which cases that we've read so far involve questions of personal jurisdiction? How is that different from choice of law? How are the two of them related? Have you considered taking Conflicts of Law?

(2) *Young* and *Boschetto* are opposites, in a sense. In *Young*, the newspaper knew where Young lived and worked, but didn't mean to do anything there. In *Boschetto*, on the other hand, the seller didn't know where the winning bidder would be from, but did expect to ship a car there (wherever it wound up being). Both of them argue that they should be immune from jurisdiction in their alleged victim's forum state. Which has the more sympathetic case? Are these two opinions correctly decided?

(3) Four of the five cases or today involve lawsuits in which all of the parties are American. Why are the parties litigating the personal-jurisdiction issue when the plaintiff could just have filed suit in the defendant's state?

(4) Internationally, the tendency is to focus on the "effects" of the defendant's conduct, and would generally to find personal jurisdiction wherever those effects were felt. How does that analysis differ from the "intent to direct" in *Young* and the "purposeful availment" in *Boschetto*. Remember the Australian defamation case, *Gutnick*? Did Australia have personal jurisdiction over Dow Jones and its reporters under an "effects" test? Under *Young* and *Boschetto*?

(5) What would John Perry Barlow say about these cases? Does he have a horse in this race? What about Jack Goldsmith and Tim Wu ? Or David Johnson and David Post?

(6) Does Orin Kerr's internal/external distinction help to make sense out of *Westside Story*? What's the internal perspective on the defendant's actions? The external perspective?

Young v. New Haven Advocate
315 F.3d 256 (4th Cir. 2002)

MICHAEL, Circuit Judge:

The question in this appeal is whether two Connecticut newspapers and certain of their staff (sometimes, the "newspaper defendants") subjected themselves to personal jurisdiction in Virginia by posting on the Internet news articles that, in the context of discussing the State of Connecticut's policy of housing its prisoners in Virginia institutions, allegedly defamed the warden of a Virginia prison. Our recent decision in *ALS Scan, Inc. v. Digital Service Consultants, Inc.*, 293 F.3d 707 (4th Cir. 2002), supplies the standard for determining a court's authority to exercise personal jurisdiction over an out-of-state person who places information on the Internet. Applying that standard, we hold that a court in Virginia cannot constitutionally exercise jurisdiction over the Connecticut-based newspaper defendants because they did not manifest an intent to aim their websites or the posted articles at a Virginia audience. Accordingly, we reverse the district court's order denying the defendants' motion to dismiss for lack of personal jurisdiction.

I.

Sometime in the late 1990s the State of Connecticut was faced with substantial overcrowding in its maximum security prisons. To alleviate the problem, Connecticut contracted with the Commonwealth of Virginia to house Connecticut prisoners in Virginia's correctional facilities. Beginning in late 1999 Connecticut transferred about 500 prisoners, mostly African-American and Hispanic, to the Wallens Ridge State Prison, a "supermax" facility in Big Stone Gap, Virginia. The plaintiff, Stanley Young, is the warden at Wallens Ridge. Connecticut's arrangement to incarcerate a sizeable number of its offenders in Virginia prisons provoked considerable public debate in Connecticut. Several Connecticut legislators openly criticized the policy, and there were demonstrations against it at the state capitol in Hartford.

Connecticut newspapers, including defendants the New Haven Advocate (the Advocate) and the Hartford Courant (the Courant), began reporting on the controversy. On March 30, 2000, the Advocate published a news article, written by one of its reporters, defendant Camille Jackson, about the transfer of Connecticut inmates to Wallens Ridge. The article discussed the allegedly harsh conditions at the Virginia prison and pointed out that the long trip to southwestern Virginia made visits by prisoners' families difficult or impossible. In the middle of her lengthy article, Jackson mentioned a class action that inmates transferred from Connecticut had filed against Warden Young and the Connecticut Commissioner of Corrections. The inmates alleged a lack of proper hygiene and medical care and the denial of religious privileges at Wallens Ridge. Finally, a paragraph at the end of the article reported that a Connecticut state senator had expressed concern about the presence of Confederate Civil War memorabilia in Warden Young's office. At about the same time the Courant published three columns, written by defendant-

reporter Amy Pagnozzi, questioning the practice of relocating Connecticut inmates to Virginia prisons. The columns reported on letters written home by inmates who alleged cruelty by prison guards. In one column Pagnozzi called Wallens Ridge a "cut-rate gulag." Warden Young was not mentioned in any of the Pagnozzi columns.

On May 12, 2000, Warden Young sued the two newspapers, their editors (Gail Thompson and Brian Toolan), and the two reporters for libel in a diversity action filed in the Western District of Virginia. He claimed that the newspapers' articles imply that he "is a racist who advocates racism" and that he "encourages abuse of inmates by the guards" at Wallens Ridge. Young alleged that the newspapers circulated the allegedly defamatory articles throughout the world by posting them on their Internet websites.

The newspaper defendants filed motions to dismiss the complaint under Federal Rule of Civil Procedure 12(b)(2) on the ground that the district court lacked personal jurisdiction over them. In support of the motions the editor and reporter from each newspaper provided declarations establishing the following undisputed facts. The Advocate is a free newspaper published once a week in New Haven, Connecticut. It is distributed in New Haven and the surrounding area, and some of its content is published on the Internet. The Advocate has a small number of subscribers, and none of them are in Virginia. The Courant is published daily in Hartford, Connecticut. The newspaper is distributed in and around Hartford, and some of its content is published on the Internet. When the articles in question were published, the Courant had eight mail subscribers in Virginia. Neither newspaper solicits subscriptions from Virginia residents. No one from either newspaper, not even the reporters, traveled to Virginia to work on the articles about Connecticut's prisoner transfer policy. The two reporters, Jackson of the Advocate and Pagnozzi of the Courant, made a few telephone calls into Virginia to gather some information for the articles. Both interviewed by telephone a spokesman for the Virginia Department of Corrections. All other interviews were done with people located in Connecticut. The two reporters wrote their articles in Connecticut. The individual defendants (the reporters and editors) do not have any traditional contacts with the Commonwealth of Virginia. They do not live in Virginia, solicit any business there, or have any assets or business relationships there. The newspapers do not have offices or employees in Virginia, and they do not regularly solicit or do business in Virginia. Finally, the newspapers do not derive any substantial revenue from goods used or services rendered in Virginia.

In responding to the declarations of the editors and reporters, Warden Young pointed out that the newspapers posted the allegedly defamatory articles on Internet websites that were accessible to Virginia residents. In addition, Young provided copies of assorted printouts from the newspapers' websites. For the Advocate, Young submitted eleven pages from newhavenadvocate.com and newmassmedia.com for January 26, 2001. The two pages from newhavenadvocate.com are the Advocate's homepage, which includes links to articles about the "Best of New Haven" and New Haven's park police. The nine pages from newmassmedia.com, a website maintained by the publishers of the Advocate, consist of classified advertising from that week's newspapers and instructions on how to submit a classified ad. The listings include advertisements for real estate rentals in New Haven and Guilford, Connecticut, for roommates wanted and tattoo services offered in Hamden, Connecticut, and for a bassist needed by a band in West Haven, Connecticut. For the Courant, Young provided nine pages from hartfordcourant.com and ctnow.com for January 26, 2001. The hartfordcourant.com homepage characterizes the website as a "source of news and entertainment in and about Connecticut." A

page soliciting advertising in the Courant refers to "exposure for your message in this market" in the "best medium in the state to deliver your advertising message." The pages from ctnow.com, a website produced by the Courant, provide news stories from that day's edition of the Courant, weather reports for Hartford and New Haven, Connecticut, and links to sites for the University of Connecticut and Connecticut state government. The website promotes its online advertising as a "source for jobs in Connecticut." The website printouts provided for January 26, 2001, do not have any content with a connection to readers in Virginia.

The district court denied the newspaper defendants' motions to dismiss, concluding that it could exercise personal jurisdiction over them under Virginia's long-arm statute, Va. Code Ann. § 8.01-328(A)(3), because "the defendants' Connecticut-based Internet activities constituted an act leading to an injury to the plaintiff in Virginia." The district court also held that the defendants' Internet activities were sufficient to satisfy the requirements of constitutional due process. With our permission the newspaper defendants are taking this interlocutory appeal. The facts relating to jurisdiction are undisputed, and the district court's decision that it has personal jurisdiction over these defendants presents a legal question that we review de novo. *See Christian Sci. Bd. of Dirs. of the First Church of Christ, Scientist v. Nolan*, 259 F.3d 209, 215 (4th Cir. 2001).

II.

A.

A federal court may exercise personal jurisdiction over a defendant in the manner provided by state law. *See ESAB Group, Inc. v. Centricut, Inc.*, 126 F.3d 617, 622 (4th Cir. 1997); Fed. R. Civ. P. 4(k)(1)(A). Because Virginia's long-arm statute extends personal jurisdiction to the extent permitted by the Due Process Clause, *see English & Smith v. Metzger*, 901 F.2d 36, 38 (4th Cir. 1990), "the statutory inquiry necessarily merges with the constitutional inquiry, and the two inquiries essentially become one." *Stover v. O'Connell Assocs., Inc.*, 84 F.3d 132, 135-36 (4th Cir. 1996). The question, then, is whether the defendant has sufficient "minimum contacts with [the forum] such that the maintenance of the suit does not offend 'traditional notions of fair play and substantial justice.'" *Int'l Shoe Co. v. Washington*, 326 U.S. 310, 316, 90 L. Ed. 95, 66 S. Ct. 154 (1945) (quoting *Milliken v. Meyer*, 311 U.S. 457, 463, 85 L. Ed. 278, 61 S. Ct. 339 (1940)). A court may assume power over an out of-state defendant either by a proper "finding [of] specific jurisdiction based on conduct connected to the suit or by [a proper] finding [of] general jurisdiction." *ALS Scan, Inc. v. Digital Serv. Consultants, Inc.*, 293 F.3d 707, 711 (4th Cir. 2002). Warden Young argues only for specific jurisdiction, so we limit our discussion accordingly. When a defendant's contacts with the forum state "are also the basis for the suit, those contacts may establish specific jurisdiction." *Id.* at 712. In determining whether specific jurisdiction exists, we traditionally ask (1) whether the defendant purposefully availed itself of the privileges of conducting activities in the forum state, (2) whether the plaintiff's claim arises out of the defendant's forum-related activities, and (3) "whether the exercise of personal jurisdiction over the defendant would be constitutionally reasonable." *Id.* at 712. *See also Christian Sci. Bd.*, 259 F.3d at 216. The plaintiff, of course, has the burden to establish that personal jurisdiction exists over the out-of-state defendant. *Young v. FDIC*, 103 F.3d 1180, 1191 (4th Cir. 1997).

B.

We turn to whether the district court can exercise specific jurisdiction over the newspaper defendants, namely, the two newspapers, the two editors, and the two reporters. To begin with,

we can put aside the few Virginia contacts that are not Internet based because Warden Young does not rely on them. Thus, Young does not claim that the reporters' few telephone calls into Virginia or the Courant's eight Virginia subscribers are sufficient to establish personal jurisdiction over those defendants. Nor did the district court rely on these traditional contacts.

Warden Young argues that the district court has specific personal jurisdiction over the newspaper defendants (hereafter, the "newspapers") because of the following contacts between them and Virginia: (1) the newspapers, knowing that Young was a Virginia resident, intentionally discussed and defamed him in their articles, (2) the newspapers posted the articles on their websites, which were accessible in Virginia, and (3) the primary effects of the defamatory statements on Young's reputation were felt in Virginia. Young emphasizes that he is not arguing that jurisdiction is proper in any location where defamatory Internet content can be accessed, which would be anywhere in the world. Rather, Young argues that personal jurisdiction is proper in Virginia because the newspapers understood that their defamatory articles, which were available to Virginia residents on the Internet, would expose Young to public hatred, contempt, and ridicule in Virginia, where he lived and worked. As the district court put it, "the defendants were all well aware of the fact that the plaintiff was employed as a warden within the Virginia correctional system and resided in Virginia," and they "also should have been aware that any harm suffered by Young from the circulation of these articles on the Internet would primarily occur in Virginia."

Young frames his argument in a way that makes one thing clear: if the newspapers' contacts with Virginia were sufficient to establish personal jurisdiction, those contacts arose solely from the newspapers' Internet-based activities. Recently, in *ALS Scan* we discussed the challenges presented in applying traditional jurisdictional principles to decide when "an out-of-state citizen, through electronic contacts, has conceptually 'entered' the State via the Internet for jurisdictional purposes." *ALS Scan*, 293 F.3d at 713. There, we held that "specific jurisdiction in the Internet context may be based only on an out-of-state person's Internet activity directed at [the forum state] and causing injury that gives rise to a potential claim cognizable in [that state]." *Id.* at 714. We noted that this standard for determining specific jurisdiction based on Internet contacts is consistent with the one used by the Supreme Court in *Calder v. Jones*, 465 U.S. 783, 79 L. Ed. 2d 804, 104 S. Ct. 1482 (1984). *ALS Scan*, 293 F.3d at 714. *Calder*, though not an Internet case, has particular relevance here because it deals with personal jurisdiction in the context of a libel suit. In *Calder* a California actress brought suit there against, among others, two Floridians, a reporter and an editor who wrote and edited in Florida a National Enquirer article claiming that the actress had a problem with alcohol. The Supreme Court held that California had jurisdiction over the Florida residents because "California [was] the focal point both of the story and of the harm suffered." *Calder*, 465 U.S. at 789. The writers' "actions were expressly aimed at California," the Court said, "and they knew that the brunt of [the potentially devastating] injury would be felt by [the actress] in the State in which she lives and works and in which the National Enquirer has its largest circulation," 600,000 copies. *Calder*, 465 U.S. at 789-90.

Warden Young argues that *Calder* requires a finding of jurisdiction in this case simply because the newspapers posted articles on their Internet websites that discussed the warden and his Virginia prison, and he would feel the effects of any libel in Virginia, where he lives and works. *Calder* does not sweep that broadly, as we have recognized. For example, in *ESAB Group, Inc. v. Centricut, Inc.*, 126 F.3d 617, 625-26 (4th Cir. 1997), we emphasized how important it is in light of *Calder* to look at whether the defendant has expressly aimed or directed its conduct toward the

forum state. We said that "although the place that the plaintiff feels the alleged injury is plainly relevant to the [jurisdictional] inquiry, it must ultimately be accompanied by the defendant's own [sufficient minimum] contacts with the state if jurisdiction . . . is to be upheld." *Id.* at 626. We thus had no trouble in concluding in *ALS Scan* that application of *Calder* in the Internet context requires proof that the out-of-state defendant's Internet activity is expressly targeted at or directed to the forum state. *ALS Scan*, 293 F.3d at 714. In *ALS Scan* we went on to adapt the traditional standard (set out in part II.A., *supra*) for establishing specific jurisdiction so that it makes sense in the Internet context. We "concluded that a State may, consistent with due process, exercise judicial power over a person outside of the State when that person (1) directs electronic activity into the State, (2) with the manifested intent of engaging in business or other interactions within the State, and (3) that activity creates, in a person within the State, a potential cause of action cognizable in the State's courts." *ALS Scan*, 293 F.3d at 714.

When the Internet activity is, as here, the posting of news articles on a website, the *ALS Scan* test works more smoothly when parts one and two of the test are considered together. We thus ask whether the newspapers manifested an intent to direct their website content — which included certain articles discussing conditions in a Virginia prison — to a Virginia audience. As we recognized in *ALS Scan*, "a person's act of placing information on the Internet"is not sufficient by itself to "subject[] that person to personal jurisdiction in each State in which the information is accessed." *Id.* at 712. Otherwise, a "person placing information on the Internet would be subject to personal jurisdiction in every State," and the traditional due process principles governing a State's jurisdiction over persons outside of its borders would be subverted. *Id. See also GTE New Media Servs. Inc. v. Bellsouth Corp.*, 339 U.S. App. D.C. 332, 199 F.3d 1343, 1350 (D.C. Cir. 2000). Thus, the fact that the newspapers' websites could be accessed anywhere, including Virginia, does not by itself demonstrate that the newspapers were intentionally directing their website content to a Virginia audience. Something more than posting and accessibility is needed to "indicate that the [newspapers] purposefully (albeit electronically) directed [their] activity in a substantial way to the forum state," Virginia. *Panavision Int'l, L.P. v. Toeppen*, 141 F.3d 1316, 1321 (9th Cir. 1998) (quotation omitted). The newspapers must, through the Internet postings, manifest an intent to target and focus on Virginia readers.

We therefore turn to the pages from the newspapers' websites that Warden Young placed in the record, and we examine their general thrust and content. The overall content of both websites is decidedly local, and neither newspaper's website contains advertisements aimed at a Virginia audience. For example, the website that distributes the Courant, ctnow.com, provides access to local (Connecticut) weather and traffic information and links to websites for the University of Connecticut and Connecticut state government. The Advocate's website features stories focusing on New Haven, such as one entitled "The Best of New Haven." In sum, it appears that these newspapers maintain their websites to serve local readers in Connecticut, to expand the reach of their papers within their local markets, and to provide their local markets with a place for classified ads. The websites are not designed to attract or serve a Virginia audience.

We also examine the specific articles Young complains about to determine whether they were posted on the Internet with the intent to target a Virginia audience. The articles included discussions about the allegedly harsh conditions at the Wallens Ridge prison, where Young was warden. One article mentioned Young by name and quoted a Connecticut state senator who reported that Young had Confederate Civil War memorabilia in his office. The focus of the

articles, however, was the Connecticut prisoner transfer policy and its impact on the transferred prisoners and their families back home in Connecticut. The articles reported on and encouraged a public debate in Connecticut about whether the transfer policy was sound or practical for that state and its citizens. Connecticut, not Virginia, was the focal point of the articles. *Cf. Griffis v. Luban*, 646 N.W.2d 527, 536 (Minn. 2002) ("The mere fact that [the defendant, who posted allegedly defamatory statements about the plaintiff on the Internet] knew that [the plaintiff] resided and worked in Alabama is not sufficient to extend personal jurisdiction over [the defendant] in Alabama, because that knowledge does not demonstrate targeting of Alabama as the focal point of the . . . statements.").

The facts in this case establish that the newspapers' websites, as well as the articles in question, were aimed at a Connecticut audience. The newspapers did not post materials on the Internet with the manifest intent of targeting Virginia readers. Accordingly, the newspapers could not have "reasonably anticipated being haled into court [in Virginia] to answer for the truth of the statements made in their articles." *Calder*, 465 U.S. at 790 (quotation omitted). In sum, the newspapers do not have sufficient Internet contacts with Virginia to permit the district court to exercise specific jurisdiction over them.

* Because the newspapers did not intentionally direct Internet activity to Virginia, and jurisdiction fails on that ground, we have no need to explore the last part of the *ALS Scan* inquiry, that is, whether the challenged conduct created a cause of action in Virginia. *See ALS Scan*, 293 F.3d at 714.

We reverse the order of the district court denying the motions to dismiss for lack of personal jurisdiction made by the New Haven Advocate, Gail Thompson (its editor), and Camille Jackson (its reporter) and by the Hartford Courant, Brian Toolan (its editor), and Amy Pagnozzi (its reporter).

Boschetto v. Hansing
539 F. 3d 1011 (9th Cir. 2008)

BETTY B. FLETCHER, Circuit Judge:

This appeal presents a question that remains surprisingly unanswered by the circuit courts: Does the sale of an item via the eBay Internet auction site provide sufficient "minimum contacts" to support personal jurisdiction over a nonresident defendant in the buyer's forum state? Plaintiff-Appellant Paul Boschetto ("Boschetto") was the winning bidder for a 1964 Ford Galaxie sold on eBay by the Defendant-Appellee, Jeffrey Hansing ("Hansing") for $34,106. Boschetto arranged for the car to be shipped from Wisconsin to California, but upon arrival it failed to meet his expectations or the advertised description. Boschetto sued in federal court; his complaint was dismissed for lack of personal jurisdiction. We now affirm.

I. FACTUAL BACKGROUND AND PROCEDURAL HISTORY

Boschetto lives in San Francisco, California. Defendant-Appellee Jeffrey D. Hansing resides in Milton, Wisconsin. Defendants-Appellees Frank-Boucher Chrysler Dodge-Jeep, Gordie Boucher Ford and Boucher Automotive Group ("Boucher Defendants") are private corporations with their principal places of business in Wisconsin. The Boucher Defendants operate a website that advertises their auto dealerships although it is not alleged that this website was connected in

any way with the transaction at issue in this case. Hansing is an employee of one of the Boucher Defendants, Frank Boucher Chrysler Dodge-Jeep. The complaint avers that on August 1, 2005, all Defendants "owned and advertised [] a 1964 Ford Galaxie 500 XL 427/425 hp 'R Code' in awesome condition, not restored, rust free chrome in excellent condition, recently rebuilt and ready to be driven, with clear title, and a vehicle warranty number of 4E68R149127."

The car was advertised for sale on the eBay Internet auction site; a copy of a portion of the eBay listing was attached to Boschetto's complaint. The eBay listing indicated that the item was located in Janesville, Wisconsin. Boschetto bid $34,106 for the Galaxie on August 8, 2005, and was notified through eBay that same day that he was the winning bidder. Boschetto and Hansing communicated via email to arrange for delivery of the vehicle from Wisconsin to California. Boschetto ultimately hired a transport company to pick up the car in Wisconsin; it arrived in California on September 15, 2005.

Upon delivery, Boschetto discovered that the car was not an "R Code" as advertised, and noted a variety of other problems, including a motor that would not turn over, rust, and extensive dents on the body of the vehicle. Boschetto contacted eBay and Hansing in an attempt to rescind the purchase, but those efforts failed. He filed a complaint in United States District Court, Northern District of California on February 23, 2006. Boschetto alleged four state law causes of action (violation of the California Consumer Protection Act; breach of contract; misrepresentation; and fraud), and pled jurisdiction pursuant to the federal diversity statute, 28 U.S.C. § 1332(a).

All Defendants moved to dismiss based on lack of personal jurisdiction. On July 13, 2006, the district court granted the motion. . . .

II. PERSONAL JURISDICTION

We review a dismissal for lack of personal jurisdiction *de novo*. *See Myers v. Bennett Law Offices*, 238 F.3d 1068, 1071 (9th Cir. 2001). In opposition to a defendant's motion to dismiss for lack of personal jurisdiction, the plaintiff bears the burden of establishing that jurisdiction is proper. *See Sher v. Johnson*, 911 F.2d 1357, 1361 (9th Cir. 1990). If the district court decides the motion without an evidentiary hearing, which is the case here, then "the plaintiff need only make a prima facie showing of the jurisdictional facts." *Id.* (citation omitted). Absent an evidentiary hearing this court "only inquire[s] into whether [the plaintiff's] pleadings and affidavits make a prima facie showing of personal jurisdiction." *Caruth v. Int'l Psychoanalytical Ass'n*, 59 F.3d 126, 127-28 (9th Cir. 1995). Uncontroverted allegations in the plaintiff's complaint must be taken as true. *See AT & T*, 94 F.3d at 588. "Conflicts between the parties over statements contained in affidavits must be resolved in the plaintiff's favor." *Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 800 (9th Cir. 2004).

When no federal statute governs personal jurisdiction, the district court applies the law of the forum state. *See Panavision Int'l L.P. v. Toeppen*, 141 F.3d 1316, 1320 (9th Cir. 1998). California's long-arm statute is co-extensive with federal standards, so a federal court may exercise personal jurisdiction if doing so comports with federal constitutional due process. *Id.* at 1320. "For a court to exercise personal jurisdiction over a nonresident defendant, that defendant must have at least 'minimum contacts' with the relevant forum such that the exercise of jurisdiction 'does not offend traditional notions of fair play and substantial justice.'" *Schwarzenegger*, 374 F.3d at 801 (quoting *International Shoe Co. v. Washington*, 326 U.S. 310, 316, 66 S.Ct. 154, 90 L.Ed. 95 (1945)). There are

two forms of personal jurisdiction that a forum state may exercise over a nonresident defendant —general jurisdiction and specific jurisdiction. We deal here only with the latter.

A. The district court correctly dismissed Boschetto's complaint for lack of personal jurisdiction.

We apply a three-part test to determine whether the exercise of specific jurisdiction over a nonresident defendant is appropriate:

> (1) The non-resident defendant must purposefully direct his activities or consummate some transaction with the forum or resident thereof; or perform some act by which he purposefully avails himself of the privilege of conducting activities in the forum, thereby invoking the benefits and protections of its laws;
>
> (2) the claim must be one which arises out of or relates to the defendant's forum-related activities; and
>
> (3) the exercise of jurisdiction must comport with fair play and substantial justice, i.e. it must be reasonable.

Id. at 802 (citing *Lake v. Lake*, 817 F.2d 1416, 1421 (9th Cir. 1987)). The plaintiff bears the burden on the first two prongs. *Id.* If the plaintiff establishes both prongs one and two, the defendant must come forward with a "compelling case" that the exercise of jurisdiction would not be reasonable. *Id.* (quoting *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 476-78, 105 S.Ct. 2174, 85 L.Ed.2d 528 (1985)). But if the plaintiff fails at the first step, the jurisdictional inquiry ends and the case must be dismissed. *See Pebble Beach Co. v. Caddy*, 453 F.3d 1151, 1155 (9th Cir. 2006) ("[Plaintiff's] arguments fail under the first prong. Accordingly, we need not address [the remaining two prongs].").

For part one of this three-part test, we have typically analyzed cases that sound primarily in contract—as Boschetto's case does—under a "purposeful availment" standard. To have purposefully availed itself of the privilege of doing business in the forum, a defendant must have "performed some type of affirmative conduct which allows or promotes the transaction of business within the forum state." *Sher*, 911 F.2d at 1362 (internal quotation marks and citation omitted). In doing so, we are guided by the Supreme Court's admonition that the formation of a contract with a nonresident defendant is not, standing alone, sufficient to create jurisdiction. *Burger King Corp.*, 471 U.S. at 478,.

Here, Boschetto fails at step one of the test for specific jurisdiction, as the lone transaction for the sale of one item does not establish that the Defendants purposefully availed themselves of the privilege of doing business in California. The arrangement between Boschetto and Hansing which is, at bottom, a contract for the sale of a good, is insufficient to have created a substantial connection with California. Hansing (and assuming *arguendo* that they had any involvement in the transaction, the Boucher Defendants) did not create any ongoing obligations with Boschetto in California; once the car was sold the parties were to go their separate ways. Neither Boschetto's complaint nor his affidavit in opposition to dismissal point to any continuing commitments assumed by the Defendants under the contract. *Id.* Nor did performance of the contract require the Defendants to engage in any substantial business in California. On Boschetto's version of the facts, funds were sent to Wisconsin and arrangements were made to pick up the car there and have it delivered to California. This

was, as the district court observed, a "one-shot affair." *See CompuServe, Inc. v. Patterson*, 89 F.3d 1257, 1265 (6th Cir. 1996). As the Supreme Court has expressly cautioned, a contract alone does not automatically establish minimum contacts in the plaintiff's home forum. *See Burger King Corp.*, 471 U.S. at 478, 105 S.Ct. 2174; *see also Doe v. Unocal Corp.*, 248 F.3d 915, 924 (9th Cir. 2001) ("However, an individual's contract with an out-of-state party alone [cannot] automatically establish sufficient minimum contacts to support personal jurisdiction.") (internal quotation marks and citations omitted); *cf. Travelers Health Ass'n v. Commonwealth of Va.*, 339 U.S. 643, 647, 70 S.Ct. 927, 94 L.Ed. 1154 (1950) (purposeful availment found if "business activities reach out beyond one state and create continuing relationships and obligations") (emphasis added).

Ignoring the limited nature of the transaction at issue, Boschetto attaches special significance to the fact that the transaction was consummated via eBay, noting that the eBay listing could have been viewed by anyone in California (or any other state for that matter) with Internet access. But the fact that eBay was used as the conduit for this sale does not affect the jurisdictional outcome, at least not on the particular facts presented here.

In *Cybersell, Inc. v. Cybersell, Inc.*, 130 F.3d 414, 419 (9th Cir. 1997), we discussed with approval a sliding scale analysis that looks to how interactive an Internet website is for purposes of determining its jurisdictional effect. ("In sum, the common thread, well stated by the district court in *Zippo*, is that the 'likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of the commercial activity that an entity conducts over the Internet.'") (quoting *Zippo Mfg. Co. v. Zippo Dot Com*, 952 F.Supp. 1119, 1124 (W.D.Pa. 1997)). The plaintiff in *Cybersell* relied on the fact that the defendant operated a website, accessible in the forum state, that contained allegedly infringing trademarks. 130 F.3d at 416. The defendant's website advertised its services but did not allow parties to transact business via the site. *Id.* at 419. Noting the lack of interactivity on the defendant's website, the court concluded that the defendant had "done no act and [] consummated no transaction, nor has it performed any act by which it purposefully availed itself of the privilege of conducting activities, in Arizona, thereby invoking the benefits and protections of Arizona law. *Id.*

The *Cybersell* analysis, while persuasive where the contact under consideration is the website itself, is largely inapplicable in this case. Here, eBay was used to create a listing for the sale of a good. Based on a superficial application of *Cybersell*, the eBay listing process and the sale it engenders is "interactive." *Id.* (noting the lack of evidence suggesting that defendant's website resulted in any business generation). But, as the district court noted, "the issue is not whether the court has personal jurisdiction over the intermediary eBay but whether it has personal jurisdiction over an individual who conducted business over eBay." In *Cybersell* and related cases where the Internet site actually belongs to and is operated by the defendant, the nature of the website has jurisdictional significance because the website allows the defendant to maintain some ongoing contact with the forum state (as well as every other state that can access the site). *See Zippo*, 952 F.Supp. at 1125-26 ("We are being asked to determine whether Dot Com's conducting of electronic commerce with Pennsylvania residents constitutes the purposeful availment of doing business in Pennsylvania."). Here, the eBay listing was not part of broader e-commerce activity; the listing temporarily advertised a good for sale and that listing closed once the item was sold, thereby extinguishing the Internet contact for this transaction within the forum state (and every other forum).

Moreover, Boschetto does not allege that any of the Defendants are using eBay to conduct business generally. He does not allege that Defendants conduct regular sales in California (or anywhere else) via eBay. Based on his own affidavit he named the Boucher Defendants based on a "good faith belief" that Hansing may have been acting as their agent during the sale. But he does not go on to allege — on information and belief or otherwise — that either Hansing or the Boucher Defendants are regular users of the eBay sales platform to sell their cars.

This is a distinction with a difference, as the cases that have found that jurisdiction was proper based on eBay sales relied heavily on the fact that the defendant was using the platform as a broader vehicle for commercial activity. *See*, *e.g.*, *Crummey v. Morgan*, 965 So.2d 497, 500 (Ct.App.La. 2007) (evidence of two prior sales to Louisiana residents in prior year); *Dedvukaj v. Maloney*, 447 F.Supp.2d 813, 822-23 (E.D.Mich.2006) ("Although the Court's research has not disclosed any personal jurisdiction cases involving the use of eBay auctions as a commercial seller's primary marketing vehicle, it is clear from the record that Defendants' use of eBay is regular and systemic."); *Malcolm v. Esposito*, 2003 WL 23272406 at *4 (Va.Cir.Ct. Dec. 12, 2003) ("Defendants are commercial sellers of automobiles who, at the time the BMW was sold, were represented on eBay as 'power sellers' with 213 transactions.").

At bottom, the consummation of the sale via eBay here is a distraction from the core issue: This was a one-time contract for the sale of a good that involved the forum state only because that is where the purchaser happened to reside, but otherwise created no "substantial connection" or ongoing obligations there. *See McGee*, 355 U.S. at 223, 78 S.Ct. 199. The Supreme Court has, in the past, sounded a note of caution that traditional jurisdictional analyses are not upended simply because a case involves technological developments that make it easier for parties to reach across state lines. *World-Wide Volkswagen v. Woodson*, 444 U.S. 286, 293, 100 S.Ct. 580, 62 L.Ed.2d 490 (1980) ("[W]e have never accepted the proposition that state lines are irrelevant for jurisdictional purposes, nor could we, and remain faithful to the principles of interstate federalism embodied in the Constitution."). The use of eBay no doubt made it far easier to reach a California buyer, but the ease with which Boschetto was contacted does not determine whether the nature and quality of the Defendants' contacts serve to support jurisdiction. That is not to say that the use of eBay digs a virtual moat around the defendant, fending off jurisdiction in all cases. Where eBay is used as a means for establishing regular business with a remote forum such that a finding of personal jurisdiction comports with "traditional notions of fair play and substantial justice," *International Shoe Co.*, 326 U.S. at 316, 66 S.Ct. 154, then a defendant's use of eBay may be properly taken into account for purposes of establishing personal jurisdiction. *See Crummey*, 965 So.2d at 500; *Dedvukaj*, 447 F.Supp.2d at 822-23; *Malcolm*, 2003 WL 23272406 at *4. But on the facts of this case—a one-time transaction—the use of eBay as the conduit for that transaction does not have any dispositive effect on jurisdiction. . . .

III. CONCLUSION

The sale of one automobile via the eBay website, without more, does not provide sufficient "minimum contacts" to establish jurisdiction over a nonresident defendant in the forum state. . . .

AFFIRMED.

[Concurrence by Judge Rymer omitted]

TravelJungle Problem

In *TravelJungle v. Am. Airlines, Inc.*, 212 S.W.3d 841 (Tex. Ct. App. 2006), the court gave the following statement of facts:

> TravelJungle operates a website that gathers hotel, car rental, and airline flight schedules and fare information in response to internet requests from consumers. With regard to airline information, TravelJungle uses special software to gather the flight and fare information from airlines' websites and from other travel websites, such as Expedia.com and Travelocity.com. Once it obtains that information, it "assimilates and sorts the data it obtains from airline and reservation sites and presents it to the requestor." Users of TravelJungle's website search it for flight information by first choosing a departure and arrival city. The website then provides the user with several fares and schedules to choose from, which the user can then select to make reservations through TravelJungle's website.
>
> TravelJungle is registered in the United Kingdom and has its principal places of business in Germany and Bulgaria. Its servers and employees are located in Germany and Bulgaria, and it has no employees in the U.S. If a user of the website decides to book one of the flights presented by TravelJungle in response to the user's request, a TravelJungle representative in Bulgaria books the flight with the organization that it got the information from via that organization's website.
>
> According to TravelJungle, between February 2003 and June 2004, TravelJungle included appellee American Airlines, Inc.'s website, AA.com, in its search for flight schedule and fare information if American provided services between the departure and arrival cities listed in a TravelJungle user's search. TravelJungle also listed AA.com on its website as one of the sites it searched to provide this information and displayed a copy of the American logo on its website.

American Airlines has sued TravelJungle in the 96th district court of Tarrant County, a Texas state court. If TravelJungle moves to dismiss the suit for lack of personal jurisdiction, how should the court rule?

Westside *Story* Problem

The facts of this problem are based on *Amberson Holdings LLC v. Westside Story Newspaper*, 110 F. Supp. 2d 332 (D.N.J. 2000).

> Amberson Holdings is the owner of a federally registered trademark on WEST SIDE STORY and control various rights related to the famous musical of that name by Leonard Bernstein. The musical, a retelling of the Romeo and Juliet story, focuses on romance and gang conflict in mid-century New York City.
>
> The defendants own and operate a weekly newspaper in San Bernadino, California, named "Westside Story," which focuses on local community issues. The defendants have registered the domain name westsidestory.com for their web site. The web site is hosted on a server operated by the New Jersey company 9 Net Avenue, Inc., and the server is physically located in the state of New Jersey. It provides about 10,000 page views a month and offers a

link to send an email to the editors of the newspaper. There is no evidence in the record about the location of its users.

Amberson has sued the newspaper for trademark infringement in federal court in the District of New Jersey. If the newspaper moves to dismiss under F.R.C.P. 12(b)(2) for lack of personal jurisdiction, how should the court rule?

MSN Problem

The facts of this problem are drawn from *Caspi v. Microsoft Network*, 732 A. 2d 528 (N.J. Super. 1999).

Plaintiffs are four users of Microsoft's online service, MSN. Two reside in New Jersey, and one each in Ohio and New York. They have filed a complaint in New Jersey state court for fraud and breach of contract, alleging that Microsoft illegally converted their memberships to more expensive plans without notice or consent. They are seeking to have the court certify a nationwide class of approximately 1.5 similarly situated MSN users.

Microsoft is, well, Microsoft. Its corporate headquarters and main offices are located in Redmond, Washington. It has sales offices in approximately 30 states, including one in New Jersey, two in New York, and three in Ohio. It does approximately $10 billion dollars of business annually worldwide. It has moved to dismiss the complaint for lack of jurisdiction and improper venue, citing a forum selection clause in its membership agreement. The forum selection clause in the agreement reads:

> This agreement is governed by the laws of the State of Washington, USA, and you consent to the exclusive jurisdiction and venue of courts in King County, Washington in all disputes arising out of or relating to your use of MSN or your MSN membership.

As the court explained:

> Before becoming an MSN member, a prospective subscriber is prompted by MSN software to view multiple computer screens of information, including a membership agreement which contains the above clause. MSN's membership agreement appears on the computer screen in a scrollable window next to blocks providing the choices "I Agree" and "I Don't Agree." Prospective members assent to the terms of the agreement by clicking on "I Agree" using a computer mouse. Prospective members have the option to click "I Agree or "I Don't Agree" at any point while scrolling through the agreement. Registration may proceed only after the potential subscriber has had the opportunity to view and has assented to the membership agreement, including MSN's forum selection clause. No charges are incurred until after the membership agreement review is completed and a subscriber has clicked on "I Agree."

How should the court rule on Microsoft's motion to dismiss?