Be Careful What You Ask For: Reconciling a Global Internet and Local Law

Harvard Law School

Harvard Law School Public Law

Research Paper No. 60

Be Careful What You Ask For: Reconciling a Global Internet and Local Law

Jonathan Zittrain

Be Careful What You Ask For: Reconciling a Global Internet and Local Law

Jonathan Zittrain[†]

We used to speak accurately of *the* Internet, a single logical network of entities only a click away from each other, no matter how distant in physical space. That was certainly the ambitious intention of those who designed it; they sought to integrate lots of existing little networks, running on a variety of physical media, into a coherent whole.

They succeeded, and the resulting network and corresponding protocols absorbed almost every other more localized or proprietized network design effort. A globalized Internet running on open protocols meant that users could disregard both their own physical location and that of anyone they traded bits with; an occasional slow-to-respond (even while lightly-trafficked) Web site might be the only betrayal of physical distance online for the average user. Web site operators, in turn, embraced the idea that setting up a single site would expose its contents to the entire Net-connected populace, wherever it might be geographically found.

This cherished fact of Internet life promptly spawned a complementary set of problems loosely categorized as "jurisdictional." At their core lay the fact that perceived serious harm – to one's reputation, digital property, peace of mind, or computer network – could now easily originate at a distance and follow a path in between accuser and accused that traversed the physical territories of any number of sovereigns. As Internet usage has gone mainstream, the problems arising from harm-at-a-distance have intensified in tandem with the ranks of those feeling injury. Individuals complaining of libel or fraud are joined by corporations worried about stock manipulation and domain name cybersquatting, as well as governments anxious about citizens purchasing faraway goods effectively exempt from sales tax, and encountering illegal speech that is not nearly as easily controlled as that issuing from print or broadcast media. Part II of this book features essays that touch on each of these problems, some from the perspectives of those threatened by the Net's global character, others from the perspectives of those threatened by actions to redress it, such as surfers subjected to Web site filtering by governments.

In this chapter I will explain two tectonic shifts in Internet architecture that are changing the ways in which these problems are addressed, and that together are likely to make them largely evaporate. These shifts will help ease the tension between the certitudes that the Internet is global, while the imposition of regulation is almost always local. These cures for the longstanding dilemmas of Internet jurisdiction and governance eliminate the originally cherished aspects of a global Internet as well – urging us to consider the iatrogenic effects of bulldozing online activity to conform more to the boundaries of the physical world that preceded it, and explaining why, in the United States and elsewhere, there are contradictory policies emerging about the Internet's future.

[†] Jack N. and Lillian R. Berkman Assistant Professor for Entrepreneurial Legal Studies, Harvard Law School.

As the kaleidoscopic sweep of topics within this book shows, the governance of behavior on the Internet is a broad topic with meanings that vary by context. All are linked by the global Internet/local law dichotomy. To understand evolving solutions to these issues, it helps to break down the topic along lines that have represented the most persistent problems: determining the proper scope of a well-meaning sovereign's reach over a physically absent accused wrongdoer; reconciling multiple jurisdictions' laws that could be said to touch on a single Internet act; and enforcing whatever judgments are thought proper to make.

A. Personal jurisdiction: How far should a government want its legal reach to extend?

The early puzzles of Internet jurisdiction invariably began with a chestnut focusing on the location of data rather than people. Thinkers were naturally intrigued by the prospect of Internet data bouncing all over the place from one point to another, such as:

> *A, in Austria, sends a threat by email to C, who retrieves the email from America Online's computers in Virginia and reads it on her screen in California. The packets making up the email traveled by way of Great Britain before reaching the United States. Where has the threat "happened"? Can California prosecute A? Can Virginia? Where can C sue? Does Great Britain care?*

Analysts thinking of this as a new and distinctly Internet-related problem were not much deterred by the fact that such hypotheticals could be constructed without any reference to the Internet – one need only imagine the threat being carried by international post or telephone – and that a world comprising hundreds of distinct (and at times contradictory) legal systems had managed not to lapse into legal crisis because of them. Perhaps those analysts thought that the Internet made formerly rare scenarios routine and reasoned that a difference in degree can become a difference in kind. Whatever the explanation, the first jurisdictional puzzles were often based on the remarkable fact that Internet technology contemplated the movement of data to any number of physical locations at any moment, a technicality that Internet users might not bear in mind when sending an email to a next door neighbor.

Of course, the practical answer in the international arena has been clear long before the Internet: C can sue (and A can be prosecuted) wherever a jurisdiction decides it cares to exercise its power – *and* can realistically make the defendant's life worse for failing to show up to contest the case, or for showing up and losing. Many jurisdictions choose to limit their decisions on exercising power on yet further factors; they may require some contact by the absent defendant (perhaps other than the very behavior complained of) before agreeing that "personal jurisdiction" exists, or they may decide that the dispute itself must touch on that physical jurisdiction in a way that makes it especially competent to locate a tribunal there (a form of "subject matter" jurisdiction).

These are useful limits to self-impose, lest a sovereign find itself enmeshed in disputes and prosecutions thanks to the mere fact that data relating to the dispute – at base,

electrical impulses – transited that sovereign's geographic territory. This may explain why, over time, analyses regarding which countries and governmental subdivisions ought to become involved in a dispute have relied less on the facts about where data might be located or found in transit, and more on the *behavior* itself complained of, and the physical location of the parties engaging in it.

Exceptions still exist where the movement or location of bits alone has been found to matter, generally where a sovereign makes it an ideologically high priority to become involved, or where cross-jurisdictional situations are themselves a substantive enhancement to a local crime or tort. In one United States case, for example, a Worthington, Ohio man was prosecuted for illegally importing obscenity into the state because he used America Online to send an email to a minor also in Worthington, Ohio. The Ohio Supreme Court found the movement of bits from the man's computer in Ohio to America Online's computer in Virginia and back to the minor's computer in Ohio to be an importation.[1]

When passing the Anticybersquatting Consumer Protection Act,[2] allowing trademark holders to sue domain name registrants whose domain names are claimed to infringe the holders' marks, the U.S. Congress provided that in those instances where the defendant was overseas or unknown, an *in rem* action could be brought against the name itself – which, if it has any location at all, reposes as data on certain computers that index domain names.[3] As a result, the *in rem* provisions allow suit wherever the registrar or registry for the name is located. In the case of .com names, that means that a Federal court in Virginia is available to would-be plaintiffs under the Act, since the company running the .com registry is located there.[4] Thus an Austrian registering a name like goodvacations.com for use in Austria might have to answer to an American court if a claim of trademark infringement arises, with theories of jurisdiction resting on the thin reed of the fact that the data management behind the domain name takes place in the United States.

Again, these examples are the exceptions. Jurisdiction based on the movement of bits alone has typically proven too expansive for sovereigns to routinely recognize it. As demonstrated by the use of the *in rem* provisions only as a backstop should the defendant be otherwise unreachable, there are usually other paths to asserting both personal power over a defendant and a subject matter interest in a case. When those paths are lacking, chances are good that the transit of bits will not and should not interest a sovereign – except in cases where a sovereign already has practical enforcement power over a defendant and is satisfied with the slimmest of procedural pretexts to claim the right to intervene. The long-term *storage* of bits in a particular physical location might trigger interest by a government with power over that location, but so long as the storage is not inadvertent or uncontrollable by whatever entity is the source of the data in question,

---

[1] *See* State v. Maxwell, 767 N.E.2d 242, 248-50 (Ohio 2002).
[2] 15 U.S.C. §1125(d) (2003).
[3] 15 U.S.C. §1125(d)(2) (2003).
[4] 15 U.S.C. §1125(d)(2). *See also* http://www.verisign-grs.com/aboutus/.

would-be defendants can choose to store data in the most hospitable physical legal environment – while still having it available worldwide through the Internet.

The existence of the so-called Principality of Sealand brings this into perfect relief. A cyberlaw textbook author's dream, Sealand is an abandoned World War II anti-aircraft platform just off the coast of Great Britain. A man named Roy Bates claimed it for his own in the mid-60's, and cites the ambiguous outcome of some U.K. court battles over its ownership – and a failed invasion attempt by German nationals in the 70's – as evidence that it is indeed a sovereign nation.

 [5]

The most recent use to which Sealand has been put is as the home of a company called Havenco, which touts itself as providing "the world's most secure managed servers in the world's only true free market environment."[6] If the storage of data alone were the anchor for the assertion of jurisdiction, data could simply be stored somewhere, such as on Sealand, that would be out of reach of the sovereigns that might have an interest in exercising jurisdiction. Interestingly, Sealand and Havenco themselves ban the use of their servers to host child pornography – as defined by U.S. law – or to mount hacking or spamming activities.[7] This could simply reflect Prince Roy's sense of right and wrong, but no doubt also results from the fact that Sealand itself must get its network connectivity somewhere – and could be at risk of losing it should its own Internet service providers reject its activities, or be pressured by nearby governments to do so. Further, the benefits to a would-be defendant of safeguarding data there for jurisdictionally evasive purposes are limited by the defendant's location. Unless a person is willing to move to Sealand, he or she would still be within another sovereign's physical and therefore legal reach and would thus risk being personally penalized should undesired activities taking place on Sealand under the defendant's direction not cease, or sought-after data secured there not be produced.

[5] From http://www.offshore-radio.de/fleet/sealand.htm.
[6] *See* http://www.havenco.com/.
[7] *See* HavenCo's Acceptable Use Policy, http://www.havenco.com/legal/aup.html.

This is why, while intriguing from an academic standpoint, the existence of Sealand doesn't much change the nature of the jurisdiction and governance debates. It's less about where the bits themselves are, and more about where the people authoring them – and allegedly causing harm by them – are.

As a government reflects on the proper limits of its reach against a faraway defendant whose Internet activities are causing local grief, it runs into a dilemma. On the one hand, a plaintiff might claim it unfair that the sovereign would decline to intervene simply because a defendant is wholly absent, since the effects of the defendant's Internet behavior are still felt locally. On the other hand, going on an "effects" test alone suggests that anyone posting information on the Internet is unduly open to nearly any sovereign's jurisdiction, since that information could have an effect around the world. Prof. Geist's essay in this volume suggests a middle path, that of "targeting," where something more than effects, but less than physical presence, could trigger jurisdiction. That path tries to peel away many if not all extraneous governments from a scrum that could pile up around a single defendant's objectionable behavior, while preserving the prospect that jurisdictions other than the defendant's home could stake a legitimate claim to intervene. As with many middle paths, the devil lies in the details. But especially in the midst of a sea change in the fundamental global Internet/local law dilemma – one where a more localized Internet is possible thanks to geolocation technologies – such a path seems the best compromise in an inherently difficult situation.

The High Court of Australia's decision in Gutnick v. Dow Jones[8] vindicates this kind of reasoning in a case that blends personal jurisdiction with choice of law. There, an Australian businessman named Joseph Gutnick sued Dow Jones for an unflattering portrait of him published online in *Barron's*. Dow Jones asked the Australian legal system to decline to intervene, arguing that Dow Jones's United States home was the fairest place to hear the dispute. The Australian court was unpersuaded by the "pile on" argument that Gutnick could next sue the company in Zimbabwe, or Great Britain, or China. It pointed out that Gutnick himself lived in Australia, and Dow Jones quite explicitly sold subscriptions to the online *Barron's* to Australians. These facts helped Australia escape the dilemma of justifying almost any country's intervention if it was to justify its own. Without its special if not unique relationship to one party in the case, Australia may well have declined to intervene in the dispute.

Even as the pure issue of "personal jurisdiction" finds a messy lawyer's compromise, when people or companies are far away from a sovereign's physical territory – or anonymous, and therefore of unknown location – the sovereign's quandaries more typically involve reconciling its laws with those of other governments that might similarly find a right to intervene, or bareknuckle enforcement of any decrees it enacts against a faraway party once it has assured itself of its right to intervene.

[8] Dow Jones & Company, Inc. v. Gutnick (2002) 194 A.L.R. 433, [2002] H.C.A. 56.

B. Choice of law: The slowest ship in the convoy problem

In the spring of 2003 the New Yorker's Seymour Hersh wrote an article about U.S. Pentagon advisor Richard Perle.[9] Perle was quoted in the New York Sun as saying that he planned to sue over the article, and in Great Britain at that, since the British libel laws were more generous to plaintiffs than those of the United States.[10] Suppose Perle spent a lot of time in Great Britain and had reputational interests there that were threatened by Hersh's piece, and suppose further that the New Yorker sold online subscriptions to British readers? A targeted effects test for personal jurisdiction might be met, but the defendant's objections need not be grounded in a lack of authority of British courts to call it to account. Rather, the New Yorker could claim that to have to hew to British law on the Internet would be an inappropriately all-or-nothing choice by the publisher. For the online New Yorker to conform to British law would mean that Americans would be deprived of content otherwise protected by the First Amendment. In essence, the global convoy of Internet publishers operating under respective countries' motley laws would harmonize at those of the most restrictive major jurisdiction – the "slowest ship."[11]

This problem is distinct from the legal nuances of personal jurisdiction, and has been raised in several other high profile disputes. For example, Canadian firm iCraveTV sought to rebroadcast television signals over the Internet, a practice that was arguably legal in Canada at the time though illegal in the United States. Broadcasters and others brought suit in the United States.[12] Personal jurisdiction was not at issue, since at least one relevant iCraveTV executive was an American citizen in residence in Pittsburgh, Pennsylvania, and the firm had an office there.[13] What made the case interesting was the prospect that the Canadian firm could be asked to cease transmitting entirely, so long as any Americans could view their online webcast feeds. The case didn't make it past the temporary restraining order phase – iCraveTV folded not long after it lost the first skirmish[14] – but it was clear from the transcripts of oral argument that the judge was not much impressed by the prospect that iCraveTV's activities were legal in Canada, so long as there could be any American viewers of the site.[15] (The United States has long had an expansive view of its jurisdiction; just ask former Panamanian strongman Manuel Noriega.)

At the state level within the United States, the "dormant commerce clause" of the Constitution is said to proscribe state laws whose effects reach beyond state borders, even if the target of regulation is legitimate within the state. It was by way of this reasoning that a district court struck down a New York law asking Web site operators to ensure that

---

[9] Seymour M. Hersh, Lunch with the Chairman, THE NEW YORKER, Mar. 13, 2003 (posted online on Mar. 10, 2003), available at http://www.newyorker.com/fact/content/?030317fa_fact.
[10] Adam Daifallah, Perle Suing Over New Yorker Article, N.Y. SUN, Mar. 12, 2003, at National 2.
[11] James C. Goodale, The Right Forum for Richard Perle, 229 N.Y.L.J. 3 (Apr. 4, 2003).
[12] Twentieth Century Fox Film Corp. et al. v. iCraveTV, Civ. Action No. 00-121 (W.D. Pa. Feb. 8, 2000).
[13] *See id*. at ¶¶ 9-13.
[14] Motion Picture Association of America, iCraveTV Signs Settlement Agreement that Shuts Down Website, Feb. 28, 2000, available at http://www.mpaa.org/Press/iCrave_Settlement.htm.
[15] *See* Twentieth Century Fox Film Corp. et al. v. iCraveTV, Civ. Action No. 00-121 (W.D. Pa. Feb. 8, 2000), Exhibit A.

indecent content could not be viewed by minors.[16] The court's view was that every Web site operator in the country would be affected by such requirements since there was no easy way to know when a New York minor might stumble onto a given site and thereby bring its operator under the sway of New York's law.[17] States are thus compelled to limit their lawmaking when an intervention affects parties outside the state who are otherwise operating under other ground rules, even as the Federal government is not held to a comparable standard vis-à-vis the international community. This may be doctrinally inconsistent, but it's perfectly understandable in the obvious absence of a unifying global legal structure.

C. Enforcement

Even if a country finds itself competent to hear a case and apply its law, enforcement of a resulting judgment can be difficult against a faraway party if the party has no significant in-country assets or interests. Dow Jones's claimed worries about answering for defamation in Zimbabwe[18] might ring hollow here; the practical dynamics of global jurisdiction suggest that a core group of powerful countries can call outsiders to account far more readily than smaller, obscure ones can. There is some push to allow for more ready enforcement of judgments across international boundaries – converging slowly towards the idea of full faith and credit among nations as already exists among the American states – but where a given country's public policy can be shown to conflict with a fellow sovereign's judgment, the deal might not be honored. When Yahoo! faced an order from a French court threatening damages unless Yahoo! took measures to preclude French citizens from viewing online auctions of Nazi memorabilia, it obtained a declaratory judgment from an American court indicating that any finding of damages there would not be enforced in the United States.[19]

The difficulties of extraterritorial enforcement can be particularly acute for countries like China. The Chinese government has great sensitivity to Internet speech that is perceived to undermine state control, but cannot readily get countries playing host to the speech – and the speakers – to enforce adverse judgments or force a stop to the speech. However, for those looking to do business in China, and thus with something to lose there, power can be brought to bear. A number of overseas content and Internet service providers targeting Chinese audiences have joined hundreds of domestic companies in signing a "Public Pledge on Self-Discipline for China Internet Industry" by which they agree, among other things, to refrain "from producing, posting or disseminating pernicious

[16] American Library Association v. Pataki, 969 F.Supp. 160 (SDNY 1997).
[17] 969 F.Supp. 160 at 167.
[18] *See* Dow Jones & Company, Inc. v. Gutnick (2002) 194 A.L.R. 433, [2002] H.C.A. 56.
[19] Yahoo! v. La Ligue Contre Le Racisme Et l'Antisemitisme and L'Union Des Etudiants Juifs De France, 169 F.Supp. 2d 1181, 1194 (N.D. Cal. 2001).

information that may jeopardize state security and disrupt social stability, contravene laws and regulations and spread superstition and obscenity."[20]

D. Global Internet, Global Law

Each of the major problems of jurisdiction – personal jurisdiction, choice of law, and enforcement – is grounded in dilemmas arising from a global Internet cabined only by local laws. Some attempts to eliminate the dilemmas have sought to simply make for global, rather than local, law. This might be done in two general ways: making a *sui generis,* non-country-specific body of law or best practices applicable to Internet activities, or striving towards substantive harmonization among existing sovereigns' laws – along with a common set of practices for personal jurisdiction and mutual enforcement of judgments.

Creating Internet-specific law has been embraced, naturally, by Internet exceptionalists who want to see a cyberspace separate and apart from real space, and generally less regulated. This was colorfully expressed in John Perry Barlow's 1996 "Declaration of Independence for Cyberspace," demanding that the industrialized nations of the world leave cyberspace alone, since it and its denizens were so unlike any physical world counterparts.[21] "We are forming our own Social Contract," he wrote. "This governance will arise according to the conditions of our world, not yours. Our world is different."

Others refined Barlow's account by imagining not one social contract but many, a series of cyberspaces in which likeminded people could respectively gather.[22] All of these accounts are now thoroughly dated, premised on a digital divide between offline and online that less and less exists. Instead of boasting an elite, libertarian demographic at variance with the mainstream populations of the industrialized world, the Internet is less a conceptually separate space with few direct links to non-Internet life and institutions, and more a ubiquitous tool. So long as, say, someone can post messages to thousands of America Online subscribers claiming to be a person named Ken Zeran selling offensive T-shirts – providing the real, offline Ken Zeran's telephone number as a lightning rod for irate calls – it is hard to call cyberspace separate, and its idiosyncrasies something with which "real" governments should not concern themselves. Indeed, in the Zeran case,[23] an American law provided for immunities from liability for Internet publishers of others' content without parallel immunities for their physical media counterparts. This resulted in the strange situation of Zeran's suit against America Online being categorically halted, while a suit against KRXO radio – whose disc jockeys had seen the message advertising

[20] Digital Freedom Network, Public Pledge on Self-Discipline for China Internet Industry, available at http://dfn.org/voices/china/selfdiscipline.htm.
[21] John Perry Barlow, A Declaration of the Independence of Cyberspace, Feb. 8, 1996, available at http://www.eff.org/~barlow/Declaration-Final.html.
[22] David R. Johnson & David G. Post, Law and Borders: The Rise of Law in Cyberspace, 48 STAN. L. REV. 1367 (1996).
[23] Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997)

the offensive T-shirts and conveyed it on-air to equally irate radio listeners – could go forward.[24]

Internet separatism lives on today primarily in debates about the application of state sales tax to out-of-state purchases made easy by the Internet. Unless pitched as infant industry subsidization, it is hard to imagine reasons why Internet-based purchases should effectively avoid tax while purchases consummated in physical space do not.[25] The most direct account to explain the perspective of those who seek continuing moratoria on taxing Internet purchases is simply a hostility to government regulation in general and taxes specifically. This is not an incoherent position; one might seek to prevent the "pristine" territory of the Net from being ruined by an encroachment of what one sees as irreversible overregulation in "real" space. But from the point of view of the dilemmas of jurisdiction and governance, it trades in one set of fault lines – those between countries and other legal jurisdictions – for a new one, separating the physical and virtual worlds.

The most effective – if not beloved – global law scheme has so far proven to be conveniently centered on cyberspace-specific disputes, namely those over domain names. As part of its designation by the U.S. Department of Commerce to manage global domain name policy, the Internet Corporation for Assigned Names and Numbers devised a Uniform Dispute Resolution Policy for the adjudication of claims of improper registration of names in .com, .net, and .org.[26] Operating wholly independently from any one nation's trademark laws, the UDRP neatly sidesteps many of the classic jurisdictional conundrums. A faraway or unknown domain name registrant had better step forward to defend against a claim that his or her domain name infringes someone else's rights, lest he or she lose the proceeding – and the name. Enforcement is made easy since no money or behavioral change is asked of the losing respondent – the registry is simply notified of the panel's decision and transfers control over the name to the complainant without any acquiescence required of the respondent. The substantive principles under which UDRP cases are decided are vague, requiring an assessment of the "rights" and "interests" of both parties to the dispute without specifying just how those rights should be recognized or under what sovereign's system. But this has not stopped thousands of UDRP cases from going forward, and the adoption of the UDRP system by a number of additional registries operating other generic and country-specific top level domains.

To be sure, use of the UDRP does not necessarily end legal wrangling – as mentioned, the U.S. Anticybersquatting Consumer Protection Act provides its own mechanisms for seeking to complain about another's domain name registration,[27] and any other number of trademark actions launched in countries willing to hear them could trump the UDRP's

---

[24] Zeran v. Diamond Broadcasting, Inc., Nos. 98-6092 and 98-6094, Order and Judgment (10th Cir. Jan. 28, 2000).
[25] Austan Goolsbee & Jonathan Zittrain, *Evaluating the Costs and Benefits of Taxing Internet Commerce,* 52 NAT'L TAX J. 413 (1999).
[26] ICANN, Uniform Domain-Name Dispute-Resolution Policy General Information, available at http://www.icann.org/udrp/.
[27] 15 U.S.C. §1125(d) (2003).

result, whether for complainant or respondent.[28] Harold Feld's chapter in this volume speaks to many shortcomings of ICANN and its UDRP, and highlights that a "universal" law orchestrated by a handful of staffers at a non-profit corporation may be far worse than the sometimes inconsistent regulation produced by more familiar territorial sovereigns, many of whom are run according to political principles that value and integrate individual voices and votes.

Attempts to bind sovereigns' laws substantively more closely together in a world with burgeoning transborder activity continue, and to the extent they succeed some of the structural jurisdictional tensions recede. International treaties and agreements have begun to cluster, if not fully unify, countries' practices on consumer protection, intellectual property, taxation, and to some extent, privacy. But these shifts are incremental, and often the inking of a treaty – or even, within the European Union, the promulgation of a directive left for individual countries to implement – is only a starting point that tests individual countries' and cultures' mettle to actually enforce that which has been abstractly agreed to.

E. Local Internet, Local Law

The most intriguing developments in the running jurisdictional and governance debates have been those that point towards a reassertion of effective local government control over Internet usage of people within each government's territorial boundaries.

1. Local control enabled by the source of content: The "check a box" solution

The French courts have indicated an awareness of the convoy problem in the suit brought against Yahoo! for permitting online auctions featuring the display of Nazi memorabilia in claimed contravention of local law. The outcome of that case so far has France asserting its right to demand that Yahoo! cease offering certain kinds of auctions, but only after the court chartered a three-expert panel to assess the extent to which Yahoo! could implement such a ban without having to apply it to non-French residents.[29] The panel concluded that Yahoo! was in a position to more or less determine who was accessing its auctions from France and who was not, and therefore could apply the strictures of French law to French customers without depriving, say, Americans the opportunity to browse auctions of Nazi material. Firms have sprung up to offer just such geographic determinations, and while they are far from perfect, they can sort many users

[28] *See, e.g.,* Sallen v. Corinthians Licenciamentos LTDA and Desportos Licenciamentos LTDA, No. 01-1197 (1st Cir. Dec. 5, 2001).

[29] Interim Court Order, County Court of Paris, France, (Nov. 22, 2000) *available at* http://www.cdt.org/speech/international/001120yahoofrance.pdf (containing the Opinion of the Consultants Ben Laurie, Fançois Wallon and Vinton Cerf, La Ligue Contre Le Racisme Et l'Antisemitisme and L'Union Des Etudiants Juifs De France v. Yahoo!, Inc. and Yahoo France).

into territories, and require those who wish to evade the categorization to undertake some burden and inconvenience to mask their geo-identities.[30]

Search engine Google, which offers country- and language-specific variants, apparently obeys the informal requests of officials from Germany to eliminate potentially illegal sites from its google.com counterpart at google.de.[31] So far Germany does not appear to have asked Google to eliminate such sites from those presented to German-based visitors to google.com, but the notion of geographic-specific information tailoring has lodged.

Geolocation by online service providers is likely to become easier and more accurate over time. Global positioning system chips are decreasing in price and finding their ways into laptops, and commercial opportunities exist to offer services on the basis of geography – one might soon be able to step off a plane, open a laptop or handheld personal digital assistant, and find an ad for local restaurants with automatic delivery displayed on the first sponsored Web site one visits. To the extent geolocation is possible, the convoy problem described earlier in this chapter begins to melt away. Purveyors of information may object to the administrative burden of having to tailor information for multiple jurisdictions – just as opponents of nationwide collection of local state sales taxes in the U.S. point to the difficulties of mastering each state's sales tax collection and remittance rules – but that complaint is much less searing and separate from the objection that one jurisdiction's residents will be de facto subject to another's laws because of a Web site's all-or-nothing exposure to the Net's masses.

Many old-school Netizens, eager to maintain a global Internet unsusceptible to government control, were furious at their technologically savvy brethren for adverting to the possibility of geolocation in the Yahoo! France case. This led to some perhaps-chastened repudiation of the court's decision by at least two members of the panel that enabled it, Internet pioneers Ben Laurie and Vint Cerf. Laurie outright apologized, and Cerf was quoted after the decision as making the observation "that if every jurisdiction in the world insisted on some form of filtering for its particular geographic territory, the World Wide Web would stop functioning."[32] That's an overstatement in the sense that sources of content on the Web are perfectly able to tailor their information delivery on the basis of whatever demographic they can solicit or discern from those who surf their Web sites. But it is completely accurate if one believes in "World Wide" as an affirmative ideological value for the Internet, rather than a technical description of its historically undifferentiated reach.

One can imagine a framework for Internet content providers – whether large Web site operators or individual home page designers or message board posters – where prior to information going public, a set of checkboxes is presented where the publisher can indicate just where in the world the information is to be exposed. One could check or

---

[30] *See, e.g.,* Quova's Geopoint, described at http://www.quova.com/services/geopoint.html.
[31] Jonathan Zittrain & Benjamin Edelman, Localized Google search result exclusions, Oct. 2002, available at http://cyber.law.harvard.edu/filtering/google/.
[32] Mark Ward, Experts Question Yahoo Auction Ruling, BBC News, Nov. 29, 2000, available at http://news.bbc.co.uk/1/hi/sci/tech/1046548.stm.

uncheck "United States" as a whole, or select specific states. One could check or uncheck Zimbabwe, or Australia, or the European Union. Such technological flexibility, combined with varied demands by countries for providers to filter content to hew to local laws, might induce risk-averse Internet content providers to adopt a very narrow band of publishing for their work – generally asking to limit distribution to those areas where legal risk is deemed low, or at least where potential profit from the work's consumption there is thought to exceed such risk.[33] Users eager for information will then be effectively denied access to it by faraway content providers anticipating the actions of zealous local governments seeking to expand their local regulation of more traditional media into the formerly unregulable Internet space. Worse, overcautious or simply indifferent Internet content providers will omit "unimportant" countries from the list of places able to view their offerings, enhancing a digital divide even though such countries are not explicitly seeking strong control over Internet content. Indeed, the gleam of the World Wide Web would be dulled as it became simply another window into traditional content for many surfers, rather than a raucous digital free-for-all.

Such a scenario is not inevitable, however. Countries worried about being left off information providers' checkbox list could pass safe harbor legislation providing for immunity as an enticement to content providers to allow them to remain on the list of digital destinations. Or they might index their laws to those of countries that will rarely be omitted from checkbox lists – just as Sealand's ban on the hosting of child pornography is a one sentence pointer to whatever the United States has legislated on the issue. The search for "global law" might be given a strong push as countries seek to be clumped together in the minds of content providers.

2. Local control enabled near content's destination: The Pennsylvania solution

Even with the rise of technical abilities to filter the information one places on the Internet according to viewers' locations, overseas sites may still balk at abiding by local governments' demands for change. Rather than writing off, say, Saudi Arabia as an Internet destination for fear of legal liability, an online newspaper might continue to make itself available there anyway – figuring that without in-country assets or other countries willing to enforce its judgments, there is little Saudi Arabia can do to call the newspaper to account. The same reasoning may apply to individual message posters or bloggers wanting to protest China's actions in Tibet, or fly-by-night pornographers and spammers who maintain no obvious central office or corporate staffs sensitive to international legal compliance.

This may explain why some governments are focusing not on pressuring the sources of content around the world, but rather on controlling Internet service providers across

[33] For an insightful expression of this concern, and an exploration of the theories by which a country should choose to enforce another's judgment even if it would never endorse such a judgment when rendered locally in the first instance, see Molly S. Van Houweling, Enforcement of Foreign Judgments, the First Amendment and Internet Speech: Notes for the Next Yahoo! v. LICRA (2003) (on file with author).

which data transits closer to home in an attempt to localize a Web surfer's online experience.

Indeed, Saudi Arabia and China both have comprehensive nationwide schemes by which Internet destinations deemed to run afoul of local law or convention are made unavailable to resident surfers.

In Saudi Arabia, all Internet traffic in the country is routed through a proxy server at the country's Internet Services Unit, the staff of which maintains a list of sites to be filtered, acting both to apply filtering criteria promulgated by the state and on specific filtering requests from individual state agencies.[34] The fact of filtering and some general descriptions of the criteria are available on the ISU's web site,[35] and thousands of sites – including anonymizers and translators which might themselves be easy launching pads to otherwise-blocked sites – are blocked.[36]

In China, thousands of routers around the country are apparently configured to simply drop packets going to or from Internet points of presence that have earned a bad reputation with the authorities, and increasingly subtle forms of filtering – such as temporarily denying access to Google to those who run searches using sensitive keywords, like the name of president "Jiang Zemin" – can also be found.[37] Private companies offering Internet access in China have long done so on condition that they apply whatever filtering measures are asked of them by the state.

Such filtering is far from perfect, but it can drastically increase a Net surfer's burden to getting to desired information – especially when the absence of information may be subtle, as in a missing entry on a list of search results. Peer-to-peer networks can seek to frustrate such attempts by implementing technologies such as "Publius"[38], but particularly when the act of using such technologies can itself be monitored and Net users can be punished in a distinctly non-virtual way, there exists a level of resources that a state can put into Internet filtering that tips the cat-and-mouse game in favor of the cat much if not most of the time.

It's no surprise that comparatively judicially isolated countries with censorship agendas unpopular on the international stage would turn to solutions applied close to home to create an Internet in keeping with local custom. But such practices are starting to take root in other settings as well. In the United States, the state of Pennsylvania passed a law allowing the state attorney general to call a Web page to the attention of a local judge. If the judge finds probable cause that child pornography exists on that page, the attorney

---

[34] *See* the Internet Services Unit's homepage, available at http://www.isu.net.sa/index.htm.
[35] *See* the Internet Services Unit's explanation of its Content Filtering practices, available at http://www.isu.net.sa/saudi-internet/content-filtering.htm.
[36] Jonathan Zittrain & Benjamin Edelman, Documentation of Internet Filtering in Saudi Arabia, Dec. 2002, available at http://cyber.law.harvard.edu/filtering/saudiarabia/.
[37] Jonathan Zittrain & Benjamin Edelman, Empirical Analysis of Internet Filtering in China, March 2003, available at http://cyber.law.harvard.edu/filtering/china/.
[38] Information on the Publius Censorship Resistant Publishing System is available at http://cs1.cs.nyu.edu/waldman/publius.html.

general can demand that any Internet service provider with Pennsylvania customers make sure that the page is not visible to those customers. There is only one documented instance of the Pennsylvania attorney general actually invoking the formal process to demand action by a local ISP;[39] the apparent threat of legal action alone is enough to make a system of informal notifications – and corresponding blocks – take place.

Such a law reflects a clear tension in American thinking about localizing the Internet. On one hand, Christopher Cox has introduced to the U.S. Congress the Global Internet Freedom Act, described in his chapter in this very volume. It is a clarion call to make it the unabashed policy of America to maintain the Internet as a conveyor of information that repressive governments don't want their subjects to see. He sees the Internet as a precious conduit for the worldwide export of democratic ideas, and contemplates subsidizing technologies to route around local attempts at Internet censorship such as those described in this section. Such attempts, of course, are the very ones that Pennsylvania – and now other Western states and countries – are beginning to undertake to bring the Internet into line with their respective laws.

Straightforwardly argued from the accepted imposition of territorial regulation in physical space, attempts to localize the global Internet seem perfectly reasonable. This is why Jack Goldsmith's chapter of this volume is so compelling – he struggles to understand why the existence of the Internet poses any really new problems for jurisdiction and governance, and largely concludes that it doesn't, or, but for enforcement difficulties, shouldn't.

Yet Post's answer to Goldsmith resonates, too. It recognizes that information is an atomic unit of a free society, and a medium that permits such extraordinary information access and manipulation by individuals so effortlessly across distances – as speakers, browsers, searchers, and consumers – is one that can be more than a new way of shopping, checking the weather, or watching traditional television at user-selected times.

As the Internet becomes part of daily living rather than a place to visit, its rough edges are smoothed and its extremes tamed by sovereigns wanting to protect consumers, prevent network resource abuse, and eliminate speech deemed harmful. The tools are now within reach to permit sovereigns with competing rulesets to play down their differences – whether by countenancing global privatization of some Internet governance issues through organizations like ICANN, coming to new international agreements on substance and procedure to reduce the friction caused by transborder data flows, or by a "live and let live" set of localization technologies to shape the Internet to suit the respective societies it touches.

What we might gain in easing jurisdictional tensions we could stand to lose in revolutionary capacity. The point of inflection at which the World Wide Internet sits

[39] *See* September 17, 2002 Order of Court of Common Pleas of Montgomery County, Pennsylvania, In the Matter of the Application of D. Michael Fisher, Attorney General of the Commonwealth of Pennsylvania for an Order Requiring an Internet Service Provider to Remove or Disable Access to Child Pornography, (July 2002) (No. Misc 689) (on file with author).

asks us to choose which we value more – international harmony and diversity that includes censorship smacking of repression, or an unavoidable baseline of freedom of expression that permits harmful speech along with constructive speech. Can those who wish for civil liberty without child pornography and rampant copyright infringement have it both ways?

Barlow wrote: "We cannot separate the air that chokes from the air upon which wings beat."[40] But governments are likely to try. The battles to watch, then, are not abstruse jurisdictional ones that Goldsmith rightly points out as more or less settled or stale whether on or off the Internet, but rather the dueling trajectories by which we embrace the Internet's freedom and curse its anarchy, love its instantaneous, global scope and regret the refuge it offers to those who lie, cheat, and steal at a distance.

[40] John Perry Barlow, A Declaration of the Independence of Cyberspace, Feb. 8, 1996, available at http://www.eff.org/~barlow/Declaration-Final.html.