Thoughts on Internet Policy and Global Governance

Robert Litan, The Brookings Institution

Tokyo Club Meetings, October 2001

Draft: September 26, 2001

Threshold Issues: Global Governance, Harmonization, and Jurisdiction

Before addressing each of the substantive policy issues relating to the Internet that we will be discussing – taxation, IPR, competition, privacy, digital divide, and so forth – it is important for the Club to address a threshold issue that relates to any one or all of these: Should there be a call for some kind of international Internet governance mechanism, much like there is for domain name registration through ICANN (which is an independent, *non-governmental* organization)?

My own view is that since much of what is done on the Internet intersects with preexisting national laws, it would be politically impossible to establish a global Internet governance body with jurisdiction just over "Internet matters." To the extent that nations do apply different laws to Internet-related transactions or activity, that may frustrate cross-border Internet commerce, such as it is.[1]

In theory, of course, these inhibitions could be removed if nations were to harmonize their laws. I believe this to be just as politically unrealistic as some sort of global governance. However, it may be realistic to urge national governments to agree to certain common *minimum* standards or policies – discussed in more detail below.

Meanwhile, as long as national laws do remain different, issues will continue to arise over what lawyers call the "conflict of law" problem: which jurisdiction's law applies in specific circumstances? In the commercial context, as applied to the Internet, this reduces to whether the law of the seller or the buyer applies. If it is the law of the seller, then any company doing business over the Web would not need to worry about conflicting laws of other countries, since it in effect would be "exporting" the law of its country. But if companies doing business on the Web are held to the law of the buyer, or even more unsettling, to the law of those who merely browse its websites, then firms face the prospect of having to comply the laws of up to 180 countries (or however many countries wish to assert that their laws applies to foreign companies doing business on the Net).

[1] I have seen no reliable data on the extent of *cross-border* Internet commerce, which in any event, musgt be relatively small. There are some data indicating that within the United States, retail Internet commerce exceeds $20 billion, while B2B internet activity is above $100 billion. Projections made before the current downturn had total Internet commerce by 2005 exceeding $1 trillion.

The recent Yahoo case – one where the French courts required Yahoo not to maintain Nazi related material on its website for users from France -- is just one, highly visible example where a country has asserted that the law of the buyer or the browser applies.[2] If other countries follow this example (and there are states within the United States that have used similar reasoning), then this will raise the costs of all companies offering to do business globally over the Internet. At a minimum, they will have to use the "geocoding" technology that Yahoo has now been forced to use, in order to identify the countries of those who visit their websites. In addition, companies must have up-to-date knowledge of the laws of other countries and tailor their websites and commercial policies accordingly. Third party vendors surely will arise to assist in compliance, but clearly a system of "buyer's law applies" will impose costs on all firms that are engaged in cross-border commerce on the Net (unless they maintain no foreign presence, and thus cannot be sued in foreign courts).

Of course, it should be noted vendors in the "real" or "non-virtual" world must comply with local laws. When a US company wants to sell a product or service in Europe or Japan, it must comply with local law. So why worry about the conflicts problem on the Net?

The major answer is that it can be difficult for vendors to know the residence of their users. Although this is not a problem where the buyer wants a physical item shipped to his country (and thus reveals his address), identification can be a problem when websites sell digitally transmitted services and content, even with the latest geocoding technologies, which are still imperfect (an expert commissioned by the French court in the Yahoo case testified that this technology currently can identify only about 70% of all website visitors). The same is true when it comes to identifying the country of those who simply browse at a given website.

As a result, what is a web vendor or website operator to do when it can't identify the source country of a customer or a visitor to its site and still wants to engage in cross-border business activity? Several solutions could help:

1. Assuming that underlying national laws are not going to be harmonized any time soon, one answer is for any relevant group of countries to agree to the following: that vendors from foreign jurisdictions and other websites maintained on servers outside any country's borders would be immune from suit (by private or public authorities) for not complying with any of the country's laws if the website's content is written in a foreign language (thus implying that the website is not targeting users of other countries), or if written in the language of the browser's or user's country, the operator of the website uses other means to make clear it is not soliciting business or use from foreign customers -- for example, by not shipping goods to addresses in the foreign country; or at least by warning that it will not accept orders for digitally transmitted content from users who identify themselves as from another country. In the case of digital transmissions, the international

[2] Yahoo is contesting the enforceability of the order of the French court in US federal court.

agreement could specify that immunity only applies where the vendor employs reasonable best efforts to identify customers (such as by employing up-to-date geocoding technology) and refuses to accept orders from customers it reasonably believes to be in the foreign country. Ideally, such an agreement would also prevent governments from suing foreign companies – assuming they could assert personal jurisdiction over them – for not complying with local law with respect to mere browsers, as well as commercial customers.

2. Another, more ambitious step, would be for participating governments to agree to apply national laws to foreign website operators or foreign companies maintaining websites *only in well-specified areas or for well-specified reasons.* Examples might include Internet content that countries believe will facilitate or spread of pornography, crime, or social unrest. Countries could define the nature of each of these criteria, the broadest category being the latter one (which would permit a France to censor Yahoo because of fear of Nazism, and which would also allow China, for example, to censor Internet content in an effort to suppress free speech). Admittedly, this would permit countries that want to practice Internet censorship to do so, but it could prevent them from asserting national substantive laws in other, more purely commercial arenas – thus, in effect, allowing vendors to choose which country's law governs any transaction (presumably the vendor's home country).

3. There may be a private sector solution to at least those conflicts in laws that relate to commercial disputes (but not reaching to conflicts created by inconsistent national laws covering such matters as prohibited content). In particular, participating *companies* could agree to establish some sort of "cyber-tribunal" that at least would resolve contractual disputes relating to transactions completed on the Internet. Companies that agree to such a system – specifically, to be bound by the decisions of such an international tribunal -- could impose a small "tax" on their sales, with the funds generated through the tax used to fund the cyber-tribunal. Users who felt they were over-charged, defrauded, or some way cheated in their transaction, could present their case via the Internet to the tribunal, supplemented with formal paper records if the tribunal deemed them necessary. There may be a market incentive for companies to advertise that they belong to such an internationally recognized system because it may increase their global sales. Clearly, an advantage of this approach is that it would be purely private and not require formal government participation and agreement.

I leave it to the group to consider these and possibly other approaches to the multiple jurisdiction problem. Below, I consider two specific policy issues -- antitrust/competition policy and privacy – whose outcomes could inhibit or promote Internet commerce.

<u>Antitrust Law and Competition Policy</u>

The following two major antitrust concerns have been raised about the Internet:

1. That the development of various exchanges – especially among competitors – could result in anti-competitive effects. For example, such exchanges could promote price collusion among competitors, both in final goods markets and in markets for supplies. To the extent the exchanges become "essential facilities" for doing business, they also could boycott potential members and thereby artificially (and anti-competitively) raise their costs of doing business.

2. In the wake of the Microsoft litigation, concerns have been raised that Microsoft – especially through its new operating system XP – could develop a "chokehold" on the Internet. For example, included in XP are Microsoft's own instant messaging system, which currently is incompatible with AOL's; Microsoft's own media players; Microsoft's "passport" system which allows users to register their credit information with the company for ease of payment (which is probably more of a privacy concern than anything else, unless Microsoft starts charging a fee for this service, somehow to the detriment of the credit card companies, or retailers, who also must join the system if it is to become fully operational).

The first set of potential antitrust problems – those that concern exchanges – may be rendered somewhat irrelevant by the lack of commercial success of many exchanges so far. However, to the extent exchanges are commercially viable, the potential antitrust concerns can be resolved by the following conditions (which we could announce in some sort of joint statement), and which to my knowledge, are already being applied by the US antitrust authorities:

(1) that any prices quoted on the exchanges are "firm" (so that firms can't signal to each other what prices they *plan* to charge, as they did in the airlines reservation case that was successfully prosecuted in the United States in the early 1990s);
(2) that the exchanges be segregated from their owners such that the information in the possession of the exchange not be passed back to their owners (so as to facilitate collusion);
(3) as a corollary to (2), that the identity of individual buyers or sellers, as the case may be, and the amounts purchased, remain secret with the exchange so that competitor-owners are not easily able to facilitate collusion;
(4) ensuring that the exchanges remain open to others who want to join the exchange (on the same terms and conditions as the other members of the exchange).

What about Microsoft? It is far from clear whether our group wants to wade into this battle, which is now before the U.S. courts (that is, the remedy to Microsoft's earlier antitrust violations relating to unlawful entrenchment of its monopoly of PC operating systems) and the EU (which is investigating Microsoft's attempted monopolization of the server market and may extend its investigation into XP).

However, the group could announce its agreement on certain principles relating to the Internet and competition policy affecting telecommunications more broadly. In particular:

--that national telecommunications markets remain open to entry by foreign firms on a non-discriminatory basis

--that any remaining government-owned telecommunications firms ought to be privatized

--that governments should do their best to promote a competitive market in Internet access by not favoring any one set of providers over another or allowing any dominant ISP to engage in practices that thwart effective competition in the ISP market

An especially controversial issue now being debated in the United States and elsewhere is whether monopoly or dominant telecommunications providers should ensure "equal access" to other companies that want to provide Internet access and other telecommunications services. In the U.S., current law requires the telephone companies to provide equal access to other ISPs, whether for narrowband or broadband Internet access. However, cable companies have not been subject to the same requirement so far. Cable companies do not yet provide regular telephone service to any significant degree (as they do in the UK), but they have about 2/3 of the broadband access market in the US (the telephone companies having the other 1/3 through the provision of digital subscriber line, or DSL, service).

As a result, there is now a proverbial public policy war in the U.S. between the local telephone monopolies (the Regional Bell Operating Companies, or RBOCs), who want to be free of the equal access requirement in the broadband market, or failing that, to have the cable companies subject to that requirement (so that the playing field is level); and the cable companies, who strongly oppose any equal access requirement on the ground that they will have less incentive to make their systems Internet-compatible if they have to share their lines with competitors under a heavily regulated process.

The RBOCs are right that the playing field is unlevel: telephone companies are subject to an equal access obligation and the cable companies are not. There are two ways to respond to this concern: either free the RBOCs from their current broadband equal access obligation (no one seriously proposes doing this for regular telephone service or narrowband internet access), or subject both cable and the RBOCs to the same equal access requirement. The problem with the first alternative – freeing the RBOCs from their current equal access obligation for broadband – is that it would allow the RBOCs to eliminate the few remaining competitors they have in the broadband market (many of the others who were in the market charge that the failure of the RBOCs to provide interconnection under existing law helped drive them out of business). The RBOCs respond that if they had no equal access obligation they would have more of an incentive to respond to customers who want broadband. As a broadband customer of an RBOC, I don't take this argument seriously. If the RBOCs wanted to serve me and others who want DSL they could do a far better job than they are doing right now. So I come down on the side of requiring the RBOCs to live under an equal access regime at least until we know more about how the broadband market is developing and whether a third competitor – satellite – may come along to provide more effective competition to both the RBOCs and the cable companies.

What about then requiring cable companies to live under same equal access regime that now applies to the RBOCs? Isn't that the fair thing to do? After all, cable already has 2/3 of the broadband market as it is? I think there is a reasonable case for accepting the logic of fairness and applying equal access to the cable companies; however, I lean against it for now for two reasons: (1) the residential broadband market is in its infancy (only 6% of US households have it) and satellite/wireless may some day provide effective competition and even if they don't, there is time to regulate the cable industry if the market matures into a quasi-monopoly; (2) equal access can be difficult to administer (what exactly is equal access, especially when the underlying delivery technology is constantly changing?).

In sum, if we were to recommend any Internet-related policies toward broadband I would suggest some like the following:

--that governments attempt to ensure that are at least two technologies available for delivering broadband Internet services – cable and DSL (telephone)

--that these technologies remain in private hands

--if governments have already required one of those delivery mechanisms to provide access to other broadband at reasonable rates, that such "equal access" requirements remain in place but not necessarily be extended to the other delivery mechanism; and

--that as the broadband market matures, governments be prepared to impose equal access requirements on both delivery mechanisms if no effective alternative delivery mechanism (such as wireless or satellite) emerges.

Nonetheless, I acknowledge there is room for reasonable people to disagree on the latter issue in particular (some of us may want to impose equal access on both cable and telephone broadband).

Finally, there is the broad question whether the rapid pace of technological change and/or the "winner-take-all" nature of some high-tech markets make antitrust enforcement less relevant or less effective.

I would argue that the tendency toward natural monopoly certain doesn't make antitrust irrelevant. While antitrust should not punish firms for being successful, even for achieving a monopoly position, it should prevent and punish dominant firms from using anti-competitive means of entrenching their monopoly position. An anti-competitive act is one which cannot be justified on normal business grounds unless the firm continues to enjoy its monopoly position. Examples include forcing consumers to buy exclusively from them; or attempting to divide markets with potential or actual entrants and threatening them with punishment if they don't comply (violations involved in the Microsoft case). Other examples include the tying of the monopoly product to a separate product -- although, as the court of appeals in the Microsoft case held, determining what is one or two products in the software business is difficult and must be judged case by case, using cost-benefit criteria. What is legitimate vs. illegitimate "integration" in the software business is very difficult to determine and thus the Microsoft court was probably

right to require this to be decided case by case. As a practical matter, however, this means that dominant software companies like Microsoft are likely to have a lot of freedom in designing their future software products.

The fact that certain markets may tend toward natural monopoly should thus make antitrust enforcement officials especially vigilant to prevent abuses of monopoly power. In addition, it underscores the importance of preventing anti-competitive mergers in markets subject to monopoly or duopoly.

However, fast paced technological change does pose a problem for antitrust enforcement officials, especially in the United States, where offenses must be litigated in the courts. This is less of a problem in the EU, where the competition directorate effectively acts as both a prosecutor and a judge. The U.S. will never adopt that system, so the best that can be done in the US context is for trials to be accelerated (much like the Microsoft trial – but without the judicial bias that the appellate court found in that case)

We also could urge that US, EU and Japanese antitrust authorities do their best to coordinate their antitrust investigations and actions, both procedurally and substantively, as both the US and EU have done in the past (in many mergers and in the first phase of the Microsoft case in 1993-95).

Privacy Law

One of prerequisites for consumers and businesses to use the Internet for commercial purposes is that they have to trust it. Hence, the importance of security and privacy.

For all intents and purposes, security is a technological question and cannot be affected that much by policy – except by requirements that certain types of firms, such as banks, meet minimum security standards in order to remain in business. Otherwise, if users don't trust the security of the Internet, they won't use it. So there are market incentives for firms to produce technologically secure Internet solutions and for Internet providing firms and those that rely on the Internet to adopt such technologies.

Consumer attitudes toward privacy vary by location. Public opinion surveys consistently show that U.S. consumers would use the Internet more extensively if they had more confidence that personal information about them that is transmitted over the Net – especially their credit card companies – will not be transferred without their consent. Judging from the EU Privacy directive implemented in 1998, Europeans value their privacy on (and off) the Net just as strongly, if not more so. However, the few sources I have seen relating to Asian consumer attitudes indicate that consumers in that part of the world do not place as great an emphasis on privacy. Instead, they display more distrust of the Net because of concerns about its security.

Until the September 11 terrorist attack in the United States, there was growing sentiment, consistent with the survey data just noted, to provide more privacy on the

Internet, through a combination of public policy measures and additional technology. As it is, U.S. privacy law already is much more protective of individuals' personal information from the government (a 1974 prohibits government agencies from sharing information about individuals), while the law was somewhat patchy when it came to personal information held by private sector organizations. Roughly speaking, the U.S. laws provide different sorts of protection for especially sensitive information: such as video rental and cable TV viewing habits (such data cannot be shared); credit histories by credit bureaus (individuals must have access to these data in order to correct them); and most recently, medical data (which broadly cannot be shared without an individual's affirmative or "opt in" consent), and certain financial data (which consumers can prevent their financial institutions from sharing with unaffiliated organizations, subject to a number of exceptions).

As for the Internet, the federal government has required parental consent for websites targeting children to obtain or share personal information from them; and it (through the Federal Trade Commission) has held that once a company announces a privacy policy – i.e. to whom it will share personal data – it must stick to that policy or else commit an "unfair trade practice."

Just prior to the terrorist attack, there were a number of bills in Congress that would have extended more generic protection to users of the Internet: at a minimum, requiring all sites to provide users with notice of their privacy or personal information policies; some would require sites to offer consumers the ability to "opt out" of having their information shared with third parties; others would be even more restrictive by requiring affirmative or "opt in" consent; and others would also require some or all sites to provide users with access to data held about them.

Meanwhile, on the technological front, there are a number of sites that offer consumers the ability to browse the web anonymously, but doing so also makes it more difficult to be a repeat customer at most sites. Perhaps most significant, Microsoft's new operating system, XP will contain a version of the long-awaited P3P technology, which will allow consumers to set a "default" switch on their browser to ensure that they only do business with websites that match their privacy preferences. Clearly, this technology will not "work" without the cooperation of many websites; that is, if consumers only want to shop at sites that offer "opt outs" and there are few or no such sites, then consumers will be frustrated and many either will not shop at all or return to the existing practice of shopping everywhere.

As for Europe, the EU implemented its well-known Privacy Directive in 1998, which applies to both on and off line environments. Broadly speaking, the Directive imposes a notice and opt out obligation on all businesses, and opt in on especially sensitive data, such as financial, medical, religion, and sexual preference [this needs to be confirmed]. The Directive also threatens a data embargo against any country that does have substantially equivalent protection. For a time, it looked like Europe would impose that embargo on the U.S., but has since negotiated a "Safe Harbor" whereby US companies that essentially maintain EU like policies will not be subject to EU retaliation.

Interestingly, the EU provides stronger protection of personal information from access by private sector companies than it does from government (where the US law is basically stronger).

Again, before the September 11 attack, it is safe to say that the sentiment of US policy makers was moving in the EU's direction, but the political environment has since changed. The US has recently given the government more authority to wiretap and to allow the FBI to monitor the web browsing behavior of individuals suspected of being involved in terrorist activity. All political momentum for tightening US privacy law in the private sector context, and specifically in the on line environment, or for extending additional protections against the release of financial information to third parties, has since been halted.

Nonetheless, from the vantage of encouraging greater use of the Internet, there is a case – notwithstanding the wartime-related government oversight of Web use – for ensuring that there is at least a minimum degree of protection of personal information collected by private entitities. The rationale for this is my belief, buttressed by the available public opinion surveys toward Internet privacy referred to earlier, that more privacy protection would enhance use of the Net.

Accordingly, I propose we urge all governments do their best to ensure that websites under their jurisdiction:

--provide notice to users of what the owners of the site will do with any personal information it collects

--give users at least the ability to "opt out" of having their personal information transmitted to third parties for marketing purposes (other uses, such as those to help detect and prevent fraud, to facilitate information processing, and so forth would not be attected);

--guarantee not to transmit especially sensitive personal information to third parties unless such transmissions are essential to provide the service (such as medical information transmitted by providers to insurance companies) and unless consumers authorize such transmissions (a so-called "opt-in" requirement); countries would define what is covered by sensitive information but examples include personal financial data, and information relating to medical histories, sexual preference and religion.

--give consumers the right to access data held about them at the cost of providing such information

<u>Other Points for the Statement</u>

I have included so far only those points relevant to my assignment, but I encourage others to modify them and, of course, to supplement them with principles from the other policy areas we will be discussing in Paris.