THE BERKMAN CENTER FOR INTERNET & SOCIETY
AT HARVARD LAW SCHOOL
Charles Nesson, Director
Jonathan Zittrain, Executive Director

Testimony of Jonathan Zittrain
before the
U.S. House of Representatives
Subcommittee on Courts and Intellectual Property
Committee on the Judiciary

June 29, 2000

1563 Massachusetts Avenue • Pound Hall 511 • Cambridge, Massachusetts 02138
+1 617.495.7547 • +1 617.495.7641 (fax) • http://cyber.law.harvard.edu • cyber@law.harvard.edu

THE BERKMAN CENTER FOR INTERNET & SOCIETY
AT HARVARD LAW SCHOOL
Charles Nesson, Director
Jonathan Zittrain, Executive Director

Summary of Testimony of Jonathan Zittrain
Before the U.S. House of Representatives
Subcommittee on Courts and Intellectual Property
Committee on the Judiciary
June 29, 2000

The Internet of tomorrow will be quite different than it is right now, transforming the issues and obstacles for the federal courts and legal jurisdiction that prevail today.

I. The Internet Today: Anonymity, Lawlessness, and Individual Freedom

The current structure of the Net makes it relatively easy for a given user to remain anonymous, and for his or her communications—including information transactions—to happen without third-party constraint. For the user, this can be liberating whether or not her actions are lawful. She may largely ignore the law without fear of material consequence. Even if she is found, issues of jurisdiction across borders can imply multiple and perhaps conflicting legal regimes.

A wide spectrum of oxen are gored by the free-for-all of today's Net:

1. Commercial Interests face problems with identity theft, credit card fraud, widely disseminated leaks of sensitive company information, and outright falsehoods designed to manipulate a stock price.
2. Publishing Interests face rampant and wholesale piracy of intellectual property.
3. Individuals face anonymous threats and spam.
4. Consumers face untrustworthy online merchants.
5. Governments face and inability to limit certain illegal content and transactions.
6. All Internet users face failure of the Net caused by cyberattacks.

Start with the premise of the free flow of information and money among anonymous parties who could be anywhere, and one cannot help but end up appreciating the Internet as an instrument of anarchy: widespread freedom from the burdens of unjust, illegitimate, or simply ill-advised law, and widespread flouting of the responsibilities entailed by just, legitimate, and reasonable restrictions on behavior.

II. The Internet Tomorrow: Architectures of Control

Of course, it is not a fact of nature that the Internet more or less enables the free flow of information and money among anonymous parties who could be anywhere. The Internet was built by people, and while it has a momentum all its own, its architecture can be redefined by people—indeed, it is in the process of being fundamentally altered right now.

A. Anonymity is becoming rarer and more expensive for a user to maintain.

--Computers themselves, rather than merely "virtual" network connections, will come to have permanent serial numbers associated with them and, in typical cases, these numbers will be broadcast to interlocutors each and every instant those computers are used on the Internet.
--The advent of a common digital signature platform means that soon people will be able to assert facts about themselves—such as their identities—that can be verified with far more certainty than the signature on a legally binding check or contract.

(over)

B. Alternative paths of access to the Internet may dwindle.

> --As we move to a world of high-speed, dedicated access, user choices between ISPs may be limited. In many neighborhoods there may only be high-speed access provided by a cable television company over its hybrid fiber-coax network, or by a baby Bell over augmented copper wires. In these instances, those who are deemed to have abused the network (or others on it) can potentially be cut off without much alternative short of moving to another house, providing a powerful incentive to behave according to whatever rules are laid down.
> --Unique hardware-based serial numbers mean that a computer could be "blacklisted" on the Internet among many of its users and gatekeepers, forcing the subject of the blacklisting to purchase a new machine to continue engaging in whatever behavior resulted in inclusion on the blacklist.

Thus, commercial interests who worry about identity theft or credit card fraud will come to use digital signature technology to ensure that consumers are who they say they are. Those who wish to identify the posters of particular information on the Net-whether companies fighting alleged leaks, businesspeople reacting to alleged libel, citizens wanting to prosecute alleged physical threats, email users resenting spam, or governments wanting to prosecute (or persecute) allegedly subversive comments-will find it easier to track the posters down or at least cause a tuning out of the flow of such comments.

III. Implications of Change: Private or Public Sheriffs?

As governments are empowered, so are many private parties in a position to effect control over Internet use. A decision to refrain from formal lawmaking may itself enable this control, as can certain laws designed expressly to further private enforcement of private laws.

The most important shift, then, from today's Internet to tomorrow's, is the shift from the public to the private. A number of bottlenecks are arising within the formerly "dumb," nondiscriminatory network, and they are instruments of both public and private power. In the former category, the usual political processes through which policy is made (and, in the United States, subjected to judicial review), will determine how that control is exploited. In the latter category, we may find whole swaths of activities traditionally thought to be public now becoming private. The "streets" through which email and other data travel from sender to recipient are, after all, private, and as they become "smarter" they can become more selective about what to let through and to what to deny passage. Whether through appropriate adjustment to intellectual property laws, through judicious application of antitrust and competition doctrines, or through affirmative creation of certain open spaces and activities, not subject to many forms of private restriction-think of the common carrier or public accommodation doctrines-the real challenge to government in the coming e-era may be to prevent undue private regulation of activities, rather than simply arrive at the right level of public regulation of these activities.

Chairman Coble, Ranking Member Berman, Members of the Subcommittee:

My name is Jonathan Zittrain, and I am the executive director of the Berkman Center for Internet & Society at Harvard Law School, where I teach and study cyberlaw.

I have structured my testimony today to share some educated guesses about where the global Internet is headed, and about the social and legal impacts of the Internet as it is likely to be tomorrow. This is because I believe that the Internet of tomorrow will be quite different than it is right now, in turn transforming the issues and obstacles for the federal courts and legal jurisdiction that prevail today.

I. The Internet Today: Anonymity, Lawlessness, and Individual Freedom

The current structure of the Net makes it relatively easy for a given user to remain anonymous, and for his or her communications including information transactions to happen without third-party constraint. This can be quite liberating for the user, and in many instances quite worrisome to those who would seek to restrict that person s online behavior. After all, if he or she can t be found or identified, or her data packets blocked under particular circumstances, the fact of legal jurisdiction is merely academic: those subject to a law that bears on online behavior can readily ignore it without material consequence. Further, even the academic aspect of legal jurisdiction can seem confusing: the Internet enables parties at a distance to interact much more easily, implicating multiple and perhaps conflicting legal regimes.

If one is generally averse to government regulation, perhaps another wrench in the workings of its exercise is to be cheered.

But a wide spectrum of oxen are gored by the free-for-all of today s Net. For commercial interests generally, there are worries about identity theft and credit card fraud, as well as widely disseminated leaks of sensitive company information or outright falsehoods designed to manipulate a stock price. For publishing interests specifically, there is the rampant and wholesale piracy of intellectual property enabled by such programs as Napster, which is now wildly popular on college campuses worldwide.

For individuals generally, there exist the prospects of receipt of anonymous threatening emails or even harmless, if annoying, unsolicited spam advertisements. For consumers specifically, there is uncertainty about whether online merchants can be trusted to be who they say they are and deliver what they promise whether the merchandise be a digital or physical good.

For governments generally, there is an inability to limit certain content or transactions deemed illegal. The Chinese government objects to a broad range of speech deemed subversive; a French court is rebuffed by Yahoo! in its demand to cease allowing those on French soil to participate in auctions of Nazi memorabilia; in Quebec, the bureau of language enforcement at one point challenged certain web sites for failing to include a French alternative to English text. Here in the United States, the difficulties have typically arisen around attempts to restrict citizens access to gambling and child pornography, as well as kids access to material whose exclusion from a school library or lower shelf of a newsstand would be wholly unremarkable.

Finally, for anyone on the Internet, there is the danger difficult to quantify that someone far away could wreak havoc on the Net itself, or computers hooked up to it, through any of a number of kinds of cyberattacks.

Start with the premise of the free flow of information and money among anonymous parties who could be anywhere, and one cannot help but end up

appreciating the Internet as an instrument of anarchy: widespread freedom from the burdens of unjust, illegitimate, or simply ill-advised law, and widespread flouting of the responsibilities entailed by just, legitimate, and reasonable restrictions on behavior. Of course, I do not seek to categorize which laws fall into which category; rather I wish to emphasize the ways in which the Internet s current resistance to law s exercise amounts, depending on one s view and the circumstances, to both more freedom and more lawlessness.

If the technical architecture of the Internet were simply a fact of nature, each interest threatened by its features could attempt to deal with it, however imperfectly, through enactment of new laws, or more robust enforcement of existing laws. In the intellectual property context, for example, this subcommittee marked up the No Electronic Theft Act, which criminalized a wide swath of copyright infringement (roughly, that done merely for fun rather than profit) that had formerly been subject only to civil penalties. The FBI has run operation Innocent Images, in which agents participate in chat rooms, awaiting those who seek to traffic in child pornography and who part with enough information to permit their arrest, should they be on U.S. soil.

In other words, the Internet will have lowered the costs of some activities those depending upon communication at a distance and raised the cost of others those depending on ready surveillance and control. Certain government restrictions would be more expensive to implement and, in some cases, thus be abandoned. These would include restrictions against others sought from government court systems by private citizens: cases against defamation, harassment, threat, and fraud might be more costly to bring and less likely to result in recovery from a reachable defendant.

Work might be done at an intergovernmental (or interstate) level to clarify choice of law and forum, but if the Internet s fundamental architecture and

protocols don t change, the underlying problems of identification of lawbreakers and distance of parties will remain.

II. Towards tomorrow s Internet: Architectures of control

Of course, it is not a fact of nature that the Internet more or less enables the free flow of information and money among anonymous parties who could be anywhere. The Internet was built by people, and while it has a momentum all its own, its architecture can be redefined by people indeed, it is in the process of being fundamentally altered right now.

I will highlight some of these changes.

First: anonymity is becoming rarer and more expensive for a user to maintain.

The original Net was built by and for people in research environments. With little or no expectation of mass adoption and the concomitant use of the Net for commercial transactions it was natural enough for the architects to trust that users of the system wouldn t misrepresent their identities.

This trust was propagated through the very network itself: each computer or point of presence on the Internet needs a unique if temporary serial number, a so-called IP address, so that it can be distinguished from every other computer hooked in. These numbers, in the first instance, were distributed in large blocs by a researcher in southern California, and ultimately found their way to every machine on the Net. Those who configured the machines had them broadcast their assigned number and were trusted not to use someone else s, or an unassigned, number. There was little incentive for such behavior called IP

spoofing and engaging in it could confuse the network and even allow data intended for someone else to end up on one s own desktop.

In today s free-for-all, there exist individual Internet users who are happy to engage in IP spoofing, whether to steal another s identity, to cloak their own activities, or just to try to disrupt the network. Already the network architects have responded: nearby data routers to one s computer no longer take that computer s announcement of its IP address as fact, and most Internet configurations now see to it that numbers are automatically assigned to computers each time they re turned on by whatever service provider is granting Internet access to that computer.

Thus, as we shift from a world of modems to a world of always-on, static Internet access from home, office, and cybercafe, the network is automatically assigning unique, quasi-permanent, somewhat traceable, and difficult-to-spoof serial numbers to every user of the Net. Indeed, the next version of IP protocol so-called IPv6 anticipates that these numbers will include, as a part, a separate unique number assigned to a given computer/network card from the moment it leaves its factory. Thus computers themselves, rather than merely virtual network connections, will come to have permanent serial numbers associated with them and, in typical cases, these numbers will be broadcast to interlocutors each and every instant those computers are used on the Internet.

Further, the advent of a common digital signature platform means that soon people will be able to assert facts about themselves such as their identities that can be verified with far more certainty than the signature on a legally binding check or contract. The cost and burden of virtually carrying and proffering an I m over 18 card, or an I m a citizen of the United States and Washington, D.C. card, will drop. It will become simple to create online activities that, for whatever reason, are intended to be limited to those who meet certain

verifiable criteria, and to exclude those who cannot or will not show that they meet those criteria.

Second: alternative paths of access to the Internet may dwindle. Several factors point to this prospect. On today s Internet, access can be achieved by using a computer modem to dial the phone number of another computer it could be anywhere which is already hooked up to the Internet. Thus dial-up ISPs, or Internet service providers, are plentiful, and one can readily switch to another if there is dissatisfaction with (or a refusal to serve by) the first.

As we move to a world of high-speed, dedicated access, the choices are much fewer. In many neighborhoods there may only be high-speed access provided by a cable television company over its hybrid fiber-coax network, or by a Baby Bell over augmented copper wires. In these instances, those who are deemed to have abused the network (or others on it) can potentially be cut off without much alternative short of moving to another house, providing a powerful incentive to behave according to whatever rules are laid down.

Further, the existence of unique hardware-based serial numbers, whether on the network card as MAC codes or on the central processing chips themselves (as Intel has attempted and, for now, aborted), means that a computer could soon be blacklisted on the Internet by many of its users and gatekeepers, forcing the subject of the blacklisting to purchase a new machine in order to continue engaging in whatever behavior resulted in inclusion on the blacklist. Further still, as computer access to the Internet itself shifts towards dedicated single-use network appliances such as TV jukeboxes and shopping terminals, the opportunity to drift from appointed paths will greatly diminish.

In essence: the dumb but reliable network that is the Internet is getting smarter, and bottlenecks are now possible within it. These bottlenecks can be

used to enforce certain levels of identity, and punishment (in the form of denial of network access) should particular rules be broken.

It may be useful to revisit the issues I inventoried in Part I of this testimony in light of these shifts. Commercial interests who worry about identity theft or credit card fraud will come to use digital signature technology to ensure that consumers are who they say they are. Those who wish to identify the posters of particular information on the Net whether companies fighting alleged leaks, businesspeople reacting to alleged libel, citizens wanting to prosecute alleged physical threats, email users resenting spam, or governments wanting to prosecute (or persecute) allegedly subversive commentators will find it easier to track the posters down or at least cause a tuning out of the flow of such comments.

The effort required for piracy of intellectual property online will skyrocket with the introduction of new systems of hardware and software designed to distribute content as a service rather than a product. College students who ship too much music around even on today s networks may find their dormitory network connections shut down, as universities find themselves in the uncomfortable but technically quite possible position of policing their own networks at the behest of publishers.

Yahoo! may find it harder to credibly object to a French court that the technology simply doesn t allow French internet users to be excluded from certain auctions, and the Congress may find, for better or worse, that the Hobson s choice occasioned by the Communications Decency Act filter out certain materials from kids eyes (an impossibility on the current Net), or go to jail is suddenly quite resolvable and thus no longer unconstitutional. In a world of digital certificates, one can rather effortlessly and definitively assert that one is over 18, permitting others accurately to withhold certain Internet content from those who are not. Similarly, a particular state could more reasonably ask an

Internet gambling site to prohibit access by those unable to certify citizenship from a jurisdiction other than that state.

Finally, the recent spate of alarming cyberattacks and viruses, itself justification for the Council of Europe s Draft Convention on Cybercrime, which the United States may seek to join may be lessened as those who mount them become easier to identify and stop at the network level.

As we look towards the Internet s future, then, over time there will be less lawlessness (or, depending on one s view, less freedom) on the Net. As a practical matter, it will be easier to identify those who break a law, and to prevent certain online behaviors. Indeed, the decrease of anonymity and increase in bottlenecks on the Internet could actually enable far more thorough control on behavior than that available before the Internet existed.

Actually reaching a lawbreaker who is in a distant country for non-Net-based enforcement purposes (arrest, service of process, fines, etc.), and sorting through overlapping jurisdictional and choice of law claims, will remain challenges, but the outlines of solutions are beginning to emerge.

Traditional lawmaking bodies would do well to note some of the boundariless, quasi-private dispute resolution mechanisms springing up, and in some cases their ability to bind all relevant Net users to their outcomes. For example, many domain name controversies that would have ended up in court with corresponding questions about jurisdiction and choice of law are now resolved entirely through a uniform dispute resolution policy promulgated by ICANN, the new non-profit charged with overseeing certain functions in the prevailing domain name framework. Today, if one is to register or renew a domain name within the most popular domains (.com, .net, and .org), one must first agree to submit to a single dispute resolution procedure by which the control

of the name can be challenged, and if the challenge is successful, the name withdrawn from the use of the registrant.

This is a form of lawmaking and governance, universally applied, but largely independent of traditional lawmaking bodies. Is it a good thing or a bad thing? It depends, of course, on one s view of the substantive policies enforced by the system, and on how much one likes the current anarchy or at least overlapping and at time contradictory rules of the Net as it stands. Of course, such dispute resolution may amount to simply one more set of rules to compete with those flowing from traditional sovereigns. After all, the recent Anticybersquatting Consumer Protection Act, Pub. L. No. 106-113, is Congress s response to the very problems of trademark infringement that ICANN s uniform domain name dispute policy was designed to solve. A domain name holder might survive a claim lodged under ICANN s procedure, but this would clearly be trumped by an adverse federal court decision under the Anticybersquatting Act.

More important, the adoption of digital signature and certification technologies can defeat the idea that the Internet knows no boundaries. With them, different Internet experiences can be tailored to different users depending on such criteria as one s citizenship, age, or location. Thus, as I ve hinted above, Minnesota can seek to restrict gambling activities of its citizens without insisting that everyone else s gambling be limited; Quebec can more easily insist that those who communicate with Quebec citizens favor one language over others; governments generally can better collect transaction taxes by tracing transactions to their points of consumer origin. For better or worse, the opportunity to enact laws concerning Internet use, targeted near-perfectly only to those citizens over which the lawmaking body has actual jurisdiction, is fast approaching.

III. Implications of change: Public or private sheriffs?

What are the implications of all this for the exercise of jurisdiction by the federal courts, and more generally the exercise of government power on the Internet through law?

Just as governments are empowered to effect control over Internet use, so too are many private parties. A decision to refrain from formal lawmaking may itself enable this control, as can certain laws designed expressly to further private enforcement of private laws.

For example, Internet engineer and protocols designer Paul Vixie, tired of receiving spam email, has set up the Realtime Blackhole List. Paul s list is one of several private efforts to simply document who is engaging in the sending of unsolicited email. Network administrators can, in turn, subscribe to a list like Paul s, and with or without the knowledge of their email subscribers, decide to blackhole, i.e. delete, any email emanating from an entity on that list. Thus, if Paul s non-profit elects to blackhole someone, that person s email will not find its way to anyone with a Hotmail account, since Microsoft, which runs Hotmail, subscribes to Paul s list.

It is now possible, and through some unconfirmed reports, actual, that a commercial web site, exchanging information with affiliate sites about whom buys what, could elect not to do business with those consumers deemed to be too smart shoppers those who always have the $10 coupon for a $10.01 purchase, or who take advantage of introductory offers or loss leaders and never come back. Indeed, a web merchant might choose among customers or at least set varying prices according to any number of factors. Thus can a consumer new to a particular merchant find her transaction rejected, or subject to a much higher cost than that found by another Internet user.

The producers of popular music, in collaboration with manufacturers of hardware and software, are building systems that prevent users from copying or lending the music they wish to hear. These systems are, in turn, backed up in the United States by the Digital Millennium Copyright Act, which criminalizes those who crack systems designed to protect any work covered by copyright. Libraries, which have, thanks to copyright s first sale doctrine, found themselves able to purchase and then lend out freely copies of books, records, and CDs, may find there is no longer anything to lend: there are simply access rights to material, defined and enforced with remarkable specificity by the technological system that serves up the material.

The most important shift, then, from today s Internet to tomorrow s, is the shift from the public to the private. A number of bottlenecks are arising within the formerly dumb, nondiscriminatory network, and they can be used to effect control both through public and private means. In the former category, the usual political processes through which policy is made (and, in the United States, subjected to judicial review), will determine how that control is exploited. In the latter category, we may find whole swaths of activities traditionally thought to be public now becoming private. The streets through which email and other data travel from sender to recipient are, after all, private, and as they become smarter they can become more selective about what to let through and to what to deny passage. Whether through appropriate adjustment to intellectual property laws, through judicious application of antitrust and competition doctrines, or through affirmative creation of open spaces and activities, free of private restriction think of the common carrier or public accommodation doctrines the real challenge to government in the coming e-era may be to prevent undue private regulation of activities, rather than simply to arrive at the right level of public regulation.

Respectfully submitted,

As required by House Rule XI, clause 2(g)(4), I hereby

- certify that I have not received any federal grant, contract, or subcontract in the current and preceding two fiscal years (I do not represent the Berkman Center or Harvard University at this hearing);

- include a curriculum vitae on the following pages.

_____

Jonathan L. Zittrain