Central Points of Control and Surveillance on a "Decentralized" Net: Internet Service Providers and Privacy and Freedom of Speech Online
By Christof Demont-Heinrich

I. Introduction

The contemporary Internet found its inspiration in the Cold War. During the 1960s and 1970s United States Department of Defense personnel and academics from a number of American universities joined together to build an interlinked network of computers capable of surviving a nuclear attack. That network manifested itself in the ARPANET. Its survival capability rested not upon some elaborate new technological discovery but instead upon a brilliantly simple strategy: decentralization. The ARPANET's architects saw that a computer network which relied upon a single command center would be far too vulnerable to attack. So they built a network with not one center, but many redundant "centers". If an attack destroyed one part of the network, other sections would continue to function.

The legacy of the ARPANET is in many ways a contradictory one. If decentralization made it virtually impossible to destroy the ARPANET via a single strategic strike, it made equally difficult the control of the network from a central point. Once the network of computers was thrown open to those beyond the academic and military communities in the early 1990s others were free to take advantage of the decentralized network in a variety of ways, some of them potentially threatening to the very military (university) industrial complex that created the first place. While decentralization makes difficult singular, top-down control it does not
represent the very antithesis of control as some Net utopians have maintained. No single institution, group, individual, or government controls the contemporary Internet. Yet this does not mean that it cannot or that it is not being controlled. Despite a history rooted in decentralization, the contemporary Net is both directly and indirectly controlled and regulated in myriad ways by a wide array of players and stakeholders. Among them: national governments, courts, law enforcement agencies, international regulatory entities, computer designers and engineers, software designers, multi-national corporations and media conglomerates, advertisers, system administrators, telecommunication giants, cable providers, and Internet Service Providers (ISPs). Individuals also control and regulate the Internet: moderators patrol newsgroups and listserv newsletters, users police one another in chat rooms, and hackers "hack" the Net to a variety of ends, including the destruction and defacement of web sites posting views with which they do not agree. 1

Thus it might be said that the real legacy of ARPANET with respect to the contemporary Internet is one of a kind of widely dispersed and relatively decentralized control. It may be impossible to exercise control over the Internet from a single, centralized point. But there remain nonetheless critical points along its decentralized infrastructure through which control can be effectively and efficiently exercised. I argue in the following analysis that the ISP constitutes precisely one of these points. In bringing into sharp relief the critical role of the ISP in the contemporary architecture of the Internet, I foreground the ways in which issues of privacy and freedom of speech converge upon, and sometimes intersect, at this key technological node. I begin, in Section II, by making an argument for the ISP as a critically situated "gateway" to Internet, noting, among other things, its unique technological location and how this plays out in terms of the ways in which other Internet structure of power stakeholders are seeking to take advantage of this location. In Section III, I attempt to situate the ISP within a larger architect
of control and surveillance on the contemporary Internet. It is here that I address in detail, the way of multiple examples and legal cases, the many and complex ways in which Fourth and First Amendment issues arise at the ISP gateway. In the Section IV, the concluding section, I examine the murky legal status of the ISP in more detail. In so doing I discuss a number of different regulatory approaches and proposals which seek to more clearly define the rather murky status of the ISP -- which in the U.S. is currently defined by the FCC as an enhanced or information service provider -- and the many functions it performs. Finally, I reflect upon some of the possible implications of the regulatory and legal schemes proposed, concluding ultimately that any such scheme must foreground the integral role that the ISP plays with respect to fundamental privacy and free speech rights on the Internet.

II. The ISP As Gateway to the Internet

A. Other Internet "Players" and the Critical Position of the ISP

The ISP, which at its most basic level "provides its customers the ability to obtain online information through the Internet" (Cannon), is the gateway to the Net. One cannot get onto "Information Superhighway" without going through an ISP even if in the end one creates one's own ISP in order to do so. And it is ultimately ISPs and telecommunications and cable providers -- some of whom are also ISPs -- who form the backbone of the Internet. Some wield considerably more power than others. So, for example, AOL, MSN, and Earthlink, together account for approximately 43 percent of the U.S. Internet market (Throsberg). Furthermore, a few telecommunications giants -- Sprint, MCI Worldcom and Cable & Wireless -- control the majority of the structural backbone along which American ISPs route their traffic ("Will the Oligopoly Prevail"). It is ISPs who operate and own the servers upon which the Domain Name Service (DNS) system underlying the basic functioning of the Internet resides. One Internet analyst has called the root server and various domain servers that interact with it "the very
of the Internet, the Archimedean point on which this vast global network balances” or, alternatively, as a "passport without which passage across the border into cyberspace is impossible" (Post qtd. in Franda: 48). According to Marcus Franda, DNS servers are "sing controlling points" "that could potentially be used to choke off access to the Internet" and therefore "have enormous value in political and economic terms" (48).

That ISPs are perhaps the most critically situated point of control on the "decentral: Net has not escaped the notice of many of the other "players" who together form its comple of power. More than 40 countries restrict their citizens' Internet surfing capabilities at the le the ISP (Denning), including powerful Western democracies such as Germany. The UK has invested more than $30 million into the construction of an Internet Surveillance Center, the Government Technical Assistance Center (GTAC). Scheduled to be operable before end of the GTAC "requires local ISPs to hardwire links directly to it, thus enabling government 'se operators' to download Internet and e-mail traffic, monitor mobile phone networks, and de code encrypted messages" (Franda 160). And in the United States, the FBI has created a surveill device known as Carnivore that is attached to ISP servers.

National governments and law enforcement agencies have not been alone in recogniz that ISPs are perhaps the most critically situated points of control on the Net. Recording in officials and representatives have successfully lobbied ISPs to revoke memberships of subscribers using peer-to-peer music software programs such as Gnutella. Individuals have libel suits against ISPs hosting allegedly defamatory newsgroup postings on their servers. A U.S. law firm recently (and unsuccessfully) sued an ISP in an attempt to force it to reveal the names of anonymous posters whom it alleged had written defamatory things about its busi ISPs in the U.S. and Britain have been successfully pressured by threats and by cyber attack yanking off the web controversial sites hosted on their servers. Employers, whose corporat
intranets comprise what some computer analysts maintain is an ISP, now regularly monitor employees' Net surfing habits and read their e-mail by way of commercial snooping software. Commercial and institutional ISPs have long kept tabs on subscriber's online actions by way of server logs. Although many ISPs have implemented policies in which they state that they do not share the information they compile about subscribers, the fact that they collect and store this data makes them prime targets for those interested in acquiring it. Those among a potentially long list of "interested parties" include law enforcement agencies as well as a wide range of private businesses who stand to benefit substantially from gaining access to detailed data about individual Internet users' web surfing habits.

B. ISPs as Flow Directors, Controllers and Surveillance Points

ISPs direct and control the flow of traffic across the Net in a number of crucial ways:

- By potentially preventing subscribers from linking to particular sites;
- By taking down "objectionable" web sites on their servers;
- By deciding which newsgroups subscribers can and cannot access;
- By way of "portals," or the default page that loads onto one's browser when one logs onto the net.

In fact media critic Robert McChesney goes so far as to call ISPs and their customized portals the "killer applications" of the Internet. The statistics which McChesney cites are both revealing and persuasive. For example, American Online controls more than a third of the U.S. market. And of the 23 million AOL subscribers in the U.S., McChesney points out, a full 80 percent never venture beyond those places at which AOL's ingeniously easy-to-use portal points.

ISPs not only comprise a "choke" point for access and flow but, as many of the above examples attest, quite possibly the most critical -- and potentially efficient -- points on the net for surveillance. All users must pass through the ISP "tollbooth" each time they merge onto
Information Superhighway. And they leave behind a trail of centrally stored -- and therefore centrally accessible -- data every time they sail through this tollbooth. As the de facto arbite privacy on the Net, ISPs are being subjected to increasing pressure from various institutions, businesses, groups, interests, and, in some cases, individuals to divulge information about subscribers, limit and control their actions, and censor what subscribers can both publish and read. That this is happening is hardly surprising. But it is not simply that ISPs have been thrust by the technological legacy of the ARPANET into a sometimes unwanted and difficult role content and privacy police. They have, by way of their data collection and storage practices, turned themselves into ready-made surveillance centers which are exceedingly enticing to a variety of players and interests. Some privacy advocates have noted that ISPs do not have to collect and store data on subscribers -- although ISPs respond that they do indeed need to watch over what goes on on their network for security as well as performance reasons.

In fact it might be said that the ISP sits at the crossroads of the First and Fourth Amendments on the Net. If Internet users know that they are being watched as they surf the web, write e-mail, post messages to newsgroups, and build web sites, if they know that the electronic trail that they leave behind at their ISP is vulnerable to marketers and law enforcement agencies, they might be inclined to restrict what they say and do. In short, the threat of "chilled" speech lurks at the critically situated ISP gateway to the Net. In fact a number of court cases revolving around ISPs and the anonymity of those who posted messages to newsgroups hosted on an ISP's servers have brought into sharp relief precisely this problem.

Political dissent, too, can be threatened at the level of the ISP. Both by the kind of surveillance that it enables, for example by way of the FBI's Carnivore program, and via ISP censorship of and/or blocking of politically unpopular or controversial web sites. Such censorship, although rare, has occurred. Proponents of the Internet as the ultimate realm of
freedom and decentralization frequently point to the fact that it is virtually impossible to suppress speech on the Net in large part because there are so many ISPs. Theirs is a point that cannot easily dismissed. There are approximately 4,500 ISPs in the United States alone (Pomeroy). There is no guarantee that that number will remain so high. Trends toward concentration of ownership in other media industries could very well play themselves out with respect to ISPs. The biggest ISP players in the United States, AOL and Microsoft Network, are part of horizontally and vertically integrated multi-media corporate conglomerates. In fact some economic analysts have asserted that it is ultimately economically inefficient to have so many ISPs as exist today. But what is economically inefficient may in fact be critical to maintaining a wide spectrum of political expression on the Internet. Many media critics have argued that concentration of ownership means fewer choices and therefore leads to fewer viewpoints being expressed. It is certainly not out of the realm of possibility that in the future a few large ISP controlling virtually the entire Internet market might find that it is not in their economic interest to allow certain views to be expressed both on, and within, their domain. Indeed there is already evidence -- albeit limited evidence, which I will discuss below -- that some ISPs might be censoring materials on their networks simply because they fear it might trigger a lawsuit and result in irate subscribers fleeing to another ISP.

C. The ISP and the Tension Between Privacy and Freedom

Many scholars have highlighted the crucial and complex relationship between privacy and freedom. "The absence of surveillance and protection of privacy," writes one, "are necessary conditions for both liberal and participatory democracy" (Raab 161). However surveillance, therefore some kind of invasion of privacy, is sometimes necessary to protect freedom. "Trusted systems" advocate and author Mark Stefik contends that three things most frequently come into conflict with privacy -- national security and law enforcement, business interests, and persc
security. Much is at stake in the struggle to balance these interests. "At what point," ask Caspar Bowden and Yaman Akdeniz in a fascinating essay explaining the future of cryptography on the Internet, "does the qualitative efficiency of surveillance invalidate the democratic legitimacy used to protect?" (102). Raab is interested in general surveillance in cyberspace. Stefik, and Bowden and Akdeniz are more concerned with larger manifestations of electronic surveillance on the Internet. None of them concentrates on the unique and critical role that the ISP plays in an ever more all-encompassing regime of cyberspatial surveillance. Indeed relatively few scholars have focused on how the tension between privacy and freedom plays itself out at the gateway to the Internet.

There are currently no legal restrictions on the kind or amount of data that ISPs may collect on subscribers. Cable operators in contrast "can collect only limited information about subscribers and must tell subscribers what data are being kept" (Middleton et al. 577). Libraries have not traditionally kept track of what books one checks out. But a record of what one has "checked out" online is potentially available through the ISP. Law enforcement agents cannot open traditional mail without a warrant or court order. Yet according to multiple critics of the FBI's Carnivore surveillance device the FBI may now have the capacity to read people's electronic mail without first having to gain the legal permission to do so. Following the controversy that arose as a result of revelations that Supreme Court nominee Robert Bork had rented pornographic videos, video stores are no longer allowed to keep tabs on customers' rentals and purchases. However no such limitations exist to prevent exactly such a list of online rentals (and visits) from being compiled by one's ISP. Trips to a bomb-building site on the Net, whatever the purpose or motivation, or to the web site of a terrorist group such as Hamas are recorded by one's ISP. Hence they are potentially available for efficient access by any number...
law enforcement agencies who might be interested in such data. The list of critical -- and useful -- information compiled at the ISP gateway is long and the chance for abuse ever present.

Nor, because they are private entities, are there any sort of legal stipulations regarding ISP censorship. To point this out is not to argue implicitly for more government regulation of ISPs who, despite the emphasis here on a seeming lack of regulation, are nonetheless subject to various kinds of direct and indirect regulation. It is to underscore that the current murky legal status of ISPs could have potentially far-reaching repercussions with respect to Fourth and Amendment issues on the Internet. What constitutes a reasonable expectation of privacy for an ISP subscriber? And on what basis -- technological and/or social -- should such an expectation be determined? Because they voluntarily enter into contractual agreements with ISPs who collect online data about them, know their names and addresses, and compile and store billing information about them, should subscribers therefore have no reasonable expectation of privacy?

Is a high expectation of e-mail privacy unreasonable because packets of information are sent through numerous privately owned and maintained servers which span wide geographic expanses?

It would seem that these questions are not viewed as being of particularly great significance by many Americans. In a recent Pew Internet & American Life Project survey 68 percent of respondents said they weren't worried that someone might know what Web sites they had visited (Grimes). And in a separate Pew poll 54 percent said that they would support government snooping of electronic mail (O'Harrow). There are other indications that many Americans do not feel particularly worried about being watched online, whether that surveil manifests itself at the ISP or elsewhere. Although they are available, comparatively few Internet users take advantage of so called anonymous re-mailers which enable the encrypted transmission of electronic mail. Recently, two companies that offered anonymous Internet surfing capaci
went out of business. And a consortium of international ISPs who had provided anonymous Internet surfing has disbanded. San Diego based Anonymizer.com, which offers anonymous surfing for $50 a year, or $5 a month, has an anemic 20,000 subscribers. "People don't understand that they're being tracked and if they do they don't care very much," says one Internet security and privacy consultant (Abreau).

If questions about privacy and freedom of speech as they coalesce at the ISP gateway may not seem particularly salient to the "average American," they are of potentially far greater consequence for those at the social, cultural and political margins. For it is their views and voices and actions of dissent that could well be "choked off" or significantly stifled at the critically situated Internet node that is the ISP. This is not to say that there is not much potentially at stake for the more than 100 million Americans who regularly log on to the Internet (Pew). An increasingly sophisticated and easily searchable and cross-referenceable regime of surveillance is manifesting itself on the Net with the ISP arguably constituting one of the most important elements in that regime. Ominous scenarios have already unfolded: for example, in which the name and profile information of a subscriber was revealed by AOL to U.S. military agents seeking to determine his sexual identity.

III. The ISP and the Larger Architecture of Control and Surveillance on the Internet

A. ISPs and the Basic Technological Infrastructure of the Net

I have already argued that ISPs constitute critical gateways and operate as the traffic monitors and directors of the Internet. But not all ISPs are created equal. Some, like AOL, MSN, and Earthlink, which together account for approximately 43 percent of the U.S. Internet market (Throsberg), are larger and more powerful than others. Furthermore only a few players control the structural backbone along which American ISPs route their traffic. Three telecommunications giants, Sprint, MCI WorldCom and Cable & Wireless own approximately 75 percent of the
optic lines along which virtually all U.S. Internet traffic moves ("Will the Oligopoly Prevail")
The larger ISPs such as AOL and MSN are often referred to as "core" ISPs. They control π of the large servers and primary routers that direct traffic across the Net. Paul Milgrom et al in an economic analysis of the contemporary ISP market define a "core" ISP as "one that maintain a full Internet routing table." Routing tables consist of directories of Internet addresses which enable packets of information flowing across the Net to be directed to the appropriate destination. Routing tables are integral to an efficient and effectively functioning Internet. If are not properly maintained or go down, a large portion of the traffic flowing across the Net grind to a halt.4 In order to maintain updated routing tables, "the core ISPs maintain peering relationships with all other core ISPs" (Milgrom et al. 176). This is a different relationship that maintained between the core ISPs and smaller ISPs. Core ISPs in a peer relationship agree to route traffic from other core ISPs across their network and through their routers in exchange the right to send their network traffic through the network and routers of a fellow core ISP. In contrast "noncore ISPs typically purchase transit from a core ISP point default routes at it" (182). They do not, note Milgrom et al., possess the resources to operate and maintain the complex routers required to obtain and update full routes. While the core ISPs worry about noncore pirates who might point default routes at their network with paying, the noncore ISPs are at a potential disadvantage should the core ISPs decide to dramatically raise the rates they charge for access. In fact Milgrom et al. speculate about the possibility of a dominant core ISP emerging in the future. Under such a scenario the dominant ISP would eliminate peer relationships and charge all other ISPs potentially exorbitant access rates in order to drive them out of business. While they express concern over the potential for an ISP monopoly, Milgrom et al. implicitly push for an ISP oligopoly. The current situation in
which "there are more than 5,000 ISPs in the US," they write, "is inefficient." Furthermore, the socially optimal number of core ISPs is likely to be relatively small subset of all ISPs" (186).

The point of the above discussion of basic technological and economic structural issues is to emphasize the distinct possibility that, as has occurred in other media and telecommunications industries, the number of ISPs may shrink significantly in the future. It is also to illustrate the fact that even in the contemporary ISP market a relatively few large, core providers boast a substantial share of Internet subscribers. They, along with a handful of telecommunications providers, control the basic infrastructure of the "decentralized" Internet. That this is so has potentially profound implications for Fourth and First Amendment issues as they are evoked at the ISP. For fewer choices and concentrated power can often mean that decisions and policies implemented by a few will end up profoundly affecting the many.

B. The Fourth Amendment and the ISP

"There is sort of a dark synergy going on: The company collects the data and the government gets that data from the company. The fact that it is collected by the company voids your privacy rights."

--Lance Cottrell, President of Anonymizer, Inc.

ISPs collect data on subscribers. They know when a subscriber logs on, when she logs off, and where she goes on the Internet. They store subscriber's e-mail and host subscriber sites. They know subscribers' names, billing addresses, and phone numbers. Furthermore, Internet Service Providers (ISPs) are now gaining the power to handle web transactions on behalf of their subscribers. As subscribers purchase goods and services off the Internet, ISPs will be able to bill digital purchases automatically to their subscribers' accounts. Although this trend allows buyers to purchase digital goods without cumbersome user registration, software downloading, or disclosing credit card information, it allows the ISP to couple its knowledge of an individual's web activity detailed purchasing histories. (Gautier)

In short, key streams of information converge at the ISP. Most ISPs pledge to protect users' privacy. And some are even attempting to capitalize on public fears about privacy violation
ad campaigns. In a recent TV ad campaign, Earthlink pledged to "provide the totally anonymous Internet" for users (Olsen). Earthlink claims to know when a subscriber logs on or off its network but not where that person travels (which seemingly isn't exactly the same thing as "the totally anonymous Internet"). Furthermore, the company says that it only keeps such data for 30 days. However it notes that this data is available to law enforcement agents, should they request it fact in 1999 Earthlink became the first ISP to be forced to install the FBI's surveillance device Carnivore, also known as DCS1000. A power struggle erupted between Earthlink and the FBI over what kind of surveillance device should be attached to Earthlink's servers. It was the FBI that ultimately emerged victorious. It placed Carnivore on Earthlink's servers -- which subsequently crashed (Kahaner).\(^5\)

The "relationship" between ISPs and both government and business agents and institutions interested in their subscriber data has been the subject of criticism by privacy advocates and civil libertarians. The criticism has come despite ISP commitments to user privacy in policy statements such as AOL's "Eight Principles of Privacy." Such policies, note some privacy advocates, typically contain a qualifier that subscriber data may be disclosed in the case of "unlawful activity". Some privacy advocates also claim that ISPs too easily and quickly "roll over" when subpoenaed to hand over subscriber information. They add that while ISPs may indeed have privacy policies in place most subscribers do not have the time to read those policies and that furthermore such policies are often vague and unclear. EPIC's Sobel notes the very fact that ISPs compile data on subscribers puts them in a position where outside interests will invariably seek to access that data. "The more stuff that they collect about subscribers for commercial interests, the more interest they will generate from law enforcement who want to hold of that information," he explains (Lemos). Commercial "interests" confirm Sobel's assertion. "In many ways," writes Mark Sweiger President of the web marketing research fi
Clickstream Consulting, "web server log file records are a dream data source." This has led to suggest that ISPs stop collecting such data. "The best thing that companies can do (to protect consumer privacy) is not record information," says Richard Smith, chief technology officer the Denver-based Privacy Foundation (Olsen). Network security and traffic flow considerate aside, there exist powerful economic incentives for ISPs to compile data on subscribers. All which seems to make Smith's suggestion that they simply stop collecting data on subscribe unlikely to be heeded. While many ISPs pledge not to disclose individual or, in some cases, aggregate data on subscribers to other sources, some are forging close relationships with marketing companies such as Predictive Networks and Compete.com which collect and ana consumer data via ISPs. The data are later used in targeted market campaigns to Internet users (Olsen)

Those zeroing in on ISP data libraries are not just law enforcement agencies and marketing companies. The music recording industry is pressuring ISPs to discipline and/or, subscribers using so-called peer-to-peer (P2P) software programs such as Gnutella and Kaz. Some ISPs, including Verizon are refusing to cut off their subscribers, but others, such as Adelphia, a Pennsylvania cable company offering high speed access, are complying with the demands and terminating agreements with subscribers who use P2P software. ISPs, notes a system administrator, are the only realistic avenue for the recording industry to take on P2P. Under the Digital Millenium Copyright Act (DMCA) of 1998, ISPs are expected to remove material from subscriber web sites that appears to constitute copyright infringement. However, the DMCA generally limits ISPs from copyright infringement liability for simply transmitting information over the Internet. But the fact that ISPs are not liable for P2P software use that occurs over their network clearly has not stopped the recording industry from pressuring ISPs. Nor has it stopped many ISPs from yielding to such pressure.
1. **Subscriber Anonymity and E-mail**

ISPs have been pressured to reveal subscriber's identity in cases involving the use of e-mail as well. Three court cases -- the *United States v. McVeigh*, the *United States v. Maxwell*, and the *United States v. Hambrick* -- reveal both the complexity of Fourth Amendment issues with respect to the Internet and the critical and sometimes difficult position ISPs occupy. In *McVeigh*, the U.S. Navy pressured AOL into releasing information (AOL violated its own privacy policy in releasing the information) on McVeigh's onscreen profile. Based on the information, which revealed that McVeigh was gay, the Navy sought to discharge him under the U.S. military's "don't ask, don't tell" policy. McVeigh ultimately prevented the Navy from using its finding by invoking Section 2703 of the Electronic Communications Privacy Act of 1986 (ECPA). The section requires that "a provider of electronic communications services disclose information only if served a warrant or court order . . . or that it obtains the consent of the subscriber or custodian before disclosing personal information" (Pomeroy).

In *Maxwell*, Colonel Maxwell was convicted through "a general court-martial of service-discrediting conduct under the Uniform Code of Military Justice for transmitting obscene images via e-mail from his personal computer" (Backes). However while convicting Maxwell, the U.S. Air Force Court of Criminal Appeals ruled that transmission of information via e-mail gives rise to a reasonable expectation of privacy and it recognized "the constitutional prerequisite of a search warrant prior to conducting a search of the defendant's e-mail data" (Backes). On appeal, the Armed Forces Court of Appeals affirmed the conviction based on the legally obtained search warrant, but emphasized the finding of the lower court that the defendant had a reasonable expectation of e-mail privacy, albeit a limited one. In establishing a higher threshold for a reasonable expectation of privacy vis-à-vis e-mail than that vis-à-vis the telephone, the military courts noted that the use of passwords limit unauthorized access to an individual's message.
courts also stressed that the "insulated structure of the ISP network, the contractual privacy arrangement with the ISP and the subjective content of the messages" justified a relatively high expectation of privacy (Backes).

In Hambrick, the U.S. Court of Appeals for the Fourth Circuit delivered a ruling at odds with that rendered in Maxwell. Scott Hambrick had been convicted in a lower court for violating child pornography laws. On appeal, Hambrick argued that the FBI had violated the Fourth Amendment when it obtained information about him from his ISP under an invalid subpoena. The information eventually led to his conviction. The Court ruled that while the subpoena was not valid that it had not been used in "bad faith." The Court also ruled that Hambrick did not have a reasonable expectation of privacy given the fact that he had voluntarily released information such as his credit card number to the ISP. It cited the United States v. Miller, 425 U.S. 435 (1976) "for the proposition that an individual has no Fourth Amendment privacy interest in information voluntarily released to a third party and later conveyed to the government" ("Fourth Circuit Rejects Privacy Claim"). The Court ruled further that there was no restrictive agreement between Hambrick and his ISP, MindSpring, that would limit MindSpring's right to release his personal information to non-governmental agencies.

The case law record is clearly contradictory with regard to subscribers' expectation of privacy vis-à-vis e-mail. At best, one might, in signing up with an ISP, assume that one's e-mail will be reasonably private (although one can never know if Carnivore is running atop an ISP network server). At worst, one might assume that the privacy of one's e-mail is wholly suspect. The latter assumption, of course, has considerable implications in terms of the "chilling of speech" effect about which many privacy advocates and civil libertarians worry.

2. Workplace Snooping
System administrators running corporate intranet "ISPs" are now acting as both undercover and content police. Employer snooping of employee web surfing and e-mail via monitoring software such as LittleBrother provides a dramatic example of the extent to which high tech surveillance now encompasses the individual virtually everywhere she goes. Other workplace web monitoring software includes Elron's Internet Manager, which, among other things, can create custom reports on top sites visited and most active users as well as send alerts when company online policies are violated. Adavi Dunkirk Software's Silent Watch allows a network administrator to monitor the workings of up to 49 computers on one screen. It also records keystrokes and sends alarms when an "inappropriate" web site is visited. And Spect produces a web monitoring program which takes hundreds of snapshots per hour of web site visits recorded by employees as well as their chat room conversations. Some programs can extrapolate how much it costs for an employee to surf the Web by multiplying the number of minutes the employee spends online by the per-minute rate of his or her salary (Savage).

According to the American Management Association, 54 percent of employers were monitoring their workers' Internet connections and 38 percent were viewing their e-mail as of the fall of 2000, both perfectly legal practices (Waltner). It is revealing to note that a recent proposal by the federal court system's chief administrator to monitor the Internet communications of the judicial branch encountered such fierce opposition that the administrator was forced to shelve it. In attempting to make his case for snooping, the administrator invoked the oft used approach of accusing those who do not want to be monitored of having something to hide. He even suggested that some of the judges who opposed web monitoring simply wanted easy access to pornography (Lewis).

3. Carnivore
The FBI's Carnivore program comprises perhaps the best known example of how the critically situated ISP gateway is being tapped in order to facilitate surveillance and, as many civil liberties and privacy advocates contend, invade ISP subscriber privacy. Carnivore consists of a hardware unit that can be attached to an ISP network server and what is commonly referred to as "packet sniffing" software which "sniffs" the multiple information packets that comprise electronic mail messages. Carnivore (to which the FBI recently began referring by the more innocuous name DCS1000) can operate in two modes – a full collection mode in which it intercepts the addressing information and content of a target user's electronic communication and a "pen collection" mode in which it gathers only the addressing information associated with e-mail, web browsing, and file transfer protocol activity. The FBI contends that Title III of Omnibus Crime Control and Safe Streets Act of 1968 (OCCSSA) and the Foreign Intelligence Surveillance Act of 1978 (FISA) provide the legal authority for Carnivore's full mode surveillance. Provisions of the ECPA are cited by the FBI as providing authority for Carnivore's pen mode surveillance (Schultz). Much controversy has swirled around Carnivore's snooping capabilities and the degree to which it can be -- or will or will not be -- used in a manner such that it will not sift indiscriminately through ISP subscriber e-mail. The controversy persists despite an independent review conducted by the Illinois Institute of Technology Research Institute to ascertain Carnivore's various capabilities.7

ISPs have been largely critical of Carnivore. Concerns about the privacy of their subscribers, the Earthlink "crash," worries about security holes that placement of Carnivore on their servers could create, the fact that they can already easily, efficiently and with precision gather individual information about subscribers' actions online, and the potential for user bottlenecks inspired by Carnivore are among the primary reasons cited by ISPs for their opposition to the program (Sachs). Meanwhile the FBI has emphasized the importance of ISPs and ISP
cooperation, illustrating in dramatic fashion the radically and increasingly central role ISPs are coming to play with respect to privacy and the Fourth Amendment on the Internet. "The technical assistance of service providers in helping a law enforcement agency execute an electronic surveillance order is always important, and in many cases it is absolutely essential" contends "This is increasingly the case with the advent of advanced communication service networks such as the Internet" (Kerr).

C. The First Amendment, Censorship, and the ISP

"Since ISPs can ultimately censor and block everything that occurs over their networks, they are potent, though limited, Internet gatekeepers. They are potent in the sense that they may cont and silence all speech on their networks."

--Raymond Shih Ray Ku

I. State Action Doctrine and ISPs

Irina Dmitrieva takes a hard look at the issue of censorship by ISPs in "Will Tomorrow Be Free? Application of State Action Doctrine to Private Internet Providers." She conclude although the Constitution fails to provide adequate redress "for violations of free speech rig by private Internet providers" that neither constitutional nor statutory law but rather case la the best legal avenue whereby to ensure that ISPs protect vital free speech online. Dmitriev: positions ISPs as critical gateways and flow directors on the Net, noting that they not only provide access but, as McChesney also argues, that they tend to funnel users toward partic places and sites by way of well-designed and easy-to-use portals. She also voices concern a trend toward mergers among Internet companies that "suggests in the future only a handful private companies will control online communications" (4). Dmitrieva starts from the premise that ISPs in some respects act like a shopping mall, in other respects like a phone company in others still like a news provider. She then examines how state action doctrine -- which ho that actions by private companies may sometimes qualify as those of the state -- has been a
to those entities and discusses whether it therefore might be applied in some cases to ISPs as well. In addressing contemporary ISP court cases, Dmitrieva focuses on a *Cyber Promotions v. America Online* decision delivered by a federal district court in Pennsylvania. In its ruling, the court argued that AOL had the right to prevent unsolicited e-mail ads from reaching its customers (18). In its decision, the court defined AOL as a ‘private online company that has invested substantial sums of its own money in equipment, name, software and reputation’ ”. It did not hold as valid the Cyber argument that AOL performs a public function in providing e-mail to members. The court also ruled that AOL does not perform “any municipal power or essential public service.” Finally, it ruled that Cyber Promotions had alternative means whereby to market its services.

2. **Protests, Attacks, and Threats Lead to ISP Censorship**

Protests and threats against ISPs by various groups, political officials, cyber terrorists and individuals illustrate that the pressure to censor extends far beyond complaints from irate subscribers about alleged spam. An e-mail bomb has led a San Francisco-based ISP to remove a Basque separatist site from its servers (Denning) (the site was quickly set up on other servers), and pressure by the British and U.S. government led a U.S. ISP to shut down IRAradio.com, an online forum and outlet for the Irish Republican Army shortly after the Sept. 11th World Trade Center attacks. After being yanked off of the web for several months, the site “was re-opened with permission,” presumably from the FBI in March 2002. In a letter published on the site shortly after it was taken down in Sept. of 2001, Travis E. Fowle, “founder and CEO” of Cosmic Entertainment, noted in an apparent reference to the USA Patriot Act that,

> President Bush recently signed a law that lets the FBI, CIA & OHS seize assets ‘with any notice and/or any real un-reasonable evidence of ANY company or person that supports, or does anything that can be labeled terrorism or is found to be connected terrorism in any way or means possible.’
Fowle then asserted (without citing any specific cases) that "word has spread about several Internet companies that have had their assets seized using this new law." Fowle cited anxiety about seized assets as the main reason for shutting down IRAradio.com. He also took pains to dissociate Cosmic from terrorism and terrorists. "THE COSMIC ENTERNTAINMENT COMPANY DOES NOT AND WILL NOT SUPPORT TERRORISM OF ANY KIND," concludes the letter (author's caps).

Pressure from a state governor may have lead AOL to remove a web site on serial killers from its servers in the late 1990s contends the American Civil Liberties Union (ACLU). "I think that ISPs feel under increasing pressure from governments to censor by refusing to service controversial sites," asserts the ACLU's Barry Steinhardt in a press release on the issue posted at aclu.org. "They are reacting in the hope that they will avoid more direct government control. Interestingly no mention is made by the ACLU about the possibility that a complaint by a irate citizen (rather than a government official) might have led to removal of the site. This despite the fact that AOL indicates that it would have pulled the site "regardless of who complained."

3. ISPs, Self-Regulation, Censorship, and "Overcompensation"

Some legal scholars and other critics warn that self-regulation of the kind currently b exercised on the Net will in fact result in over-regulation of content by ISPs. "ISP's are ill-adapted to handle their role as censors: they do not know, and should not be expected or required to know, the intricacies of the law, and, thus, will err on the side of caution," asserts Amber Jene Sayle in a legal essay published in the Wisconsin International Law Journal. "As such, ISP will be censoring speech that is protected under the Constitution. Thus, the problems with regulation in a nation that adheres to the belief of free speech become apparent: unconstitutional censorship is bound to ensue." It is primarily the specter of libel suits and what Sayle descr
as "the lurking presence of governmental regulation" that will push ISPs toward censoring controversial speech, whether on message boards, in chat rooms, or on websites, she says.

Newey advances a similar argument, asserting that private censorship puts ISPs in position "overcompensate" to limit their liability. Newey extends the argument further than Sayle, asserting that subscribers might be discouraged "from pushing the limits of acceptability, the fear of having their service cut off by the ISP" (34). Newey quotes U.S. Senator Patrick Leahy to support his argument:

"Online service providers should not be forced to become private censors: If online services or individual system operators are held liable for all of their users' communications, the services will be forced to impose stringent censorship rules on users in order to limit corporate liability of the service provider. Such rules would create a chilling effect on users of interactive media …" (34)

Others have highlighted potential problems of absolving ISPs of responsibility for that which "published" on their servers. Section 230 of the Communications Decency Act (CDA) stipulates that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider" (Lidsky).

However Congress and the Courts "have broadened its ambit far beyond merely protecting 'Good Samaritan' editorial control," asserts Lyrissa Barnett Lidsky in a February 2000 Duke Law Journal article, and effectively left "Internet defamation victims with no deep pocket to sue. For example, in Lunney v. Prodigy, a New York Court of Appeals ruled that an ISP is merely a conduit for information, as opposed to a publisher, and therefore is no more responsible than a telephone company for defamatory materials transmitted over its lines. In making its ruling, court upheld a lower court decision dismissing a defamation lawsuit brought against Prodigy Services Co., by the father of a Boy Scout whose identity was usurped by an unknown imposter. The imposter posted vulgar messages in the boy's name on an electronic bulletin board and
mailed abusive, threatening and sexually explicit messages, also in the boy’s name, to the local scoutmaster (Caher).

In another law journal article, Christopher Butler contends that the courts and Congress have extended protection of ISPs too far, arguing that “if an ISP commissions and edits information content in a manner analogous to a newspaper or book publishers, it should be to the stricter ‘publisher’ (rather than ‘distributor’) standard of fault.” However, the case law record regarding ISP liability is mixed. In 1995, a Nassau County trial court held in *Stratton Oakmont v. Prodigy* that Prodigy had editorial control over the content of messages posted electronic forum and, therefore, was responsible for potentially libelous statements made by of its users. “There is still a question of whether an ISP has complete immunity for anything happens on its system,” notes one attorney who tracks Internet-related rulings (Butler).

A British case in which an ISP agreed to a 200,000 pound out-of-court settlement after failed to act on a request by an individual to remove libelous materials from one of its newsgroups seemingly underscores the very real danger that libel suits or the threat of libel against ISPs could be wielded as indiscriminate tools of censorship. In this particular case, the litigant successfully pressured a second ISP into shutting down the web site for the Campaign Against Censorship of the Internet in Britain (CACIB), complaining about the site’s coverage of the case above. The ISP that hosted the CACIB site explained that “the costs of defending a potential libel action would be prohibitive even though a defense is most likely to be success (“Challenge to ISP Censorship”). Finally, it was in part the threat of potentially debilitating suits aimed at individual -- and therefore vulnerable -- ISPs that motivated the formation of the now defunct Zero Knowledge Systems, the consortium of ISPs who sought to provide anonymous web access, surfing and publishing. “ISPs can’t afford to fight,” one of the consortium members at the time it was founded (Zelnick).
4. ISP Censorship Issues in Germany and France

In an example which dramatically illustrates the apparent validity of Sayle's assertion “the lurking presence of government regulation” is inspiring ISP censorship, in Germany, where Nazi and other white supremacist materials are illegal, a group of ISPs recently launched an online hotline called NewsWatch to take reports of suspected illegal postings to German newsgroups. Under the NewsWatch action plan, information about material judged to be illegal is handed over to the appropriate ISP, which then deletes the material from the Internet. The NewsWatch project manager explained that the self-regulation is an attempt to avoid additional intervention by the German government (“German ISPs Seek To Curb Illegal Newsgroup Content”). In fact NewsWatch is associated with a European-wide initiative called Internet Hotline Providers in Europe (INHOPE) which is sponsored by the European Commission. If NewsWatch is given a tip on an ISP based outside of Germany, it can pass the information on to the hotline organization of the appropriate country.

France too has seen increasing pressure placed on ISPs to regulate content. In a well publicized case last year, a French judge ordered Yahoo to block French users from accessing auction areas that included Nazi memorabilia, which is illegal in France (“French ISPs Resist Blocking Racist Web Site”). However a U.S. District Court later ruled that Yahoo should not be subject to the French court's ruling, contending that French law does not trump U.S. free expression of rights. More recently, the same French judge who ruled that Yahoo needed to block the Nazi memorabilia site ruled in a separate case that French ISPs should not be forced to block French users from viewing online hate speech generated by the Front14.org web site, which was hosted on a U.S. server. The site has been brought down by hackers. However a representative for the International Action for Justice group that brought the case against French ISPs said that if the Web site were to resurface, it might take the case to a French appeals court...
The above cases dramatically illustrate the sheer complexity of free speech issues on the Net and underscore the fact the ISPs are becoming perhaps the most critically situate players in content regulation of the Net.

D. When the First and Fourth Amendments Intersect at the ISP

While this analysis has thus far highlighted instances where freedom of speech and privacy for the most part bear down separately upon the ISP, issues of privacy and freedom speech sometimes intersect at the ISP as well -- with potentially profound implications for dissent. In a recent case in California, a disgruntled employee of the Orange County Register created a web site on AOL called “The Orange County Unregister” mocking the newspaper. The newspaper brought suit against AOL, relying primarily on a claim of trademark infringement. It then had a subpoena served on AOL in an attempt to force it to reveal the identity of the web site’s author. AOL complied and the web site was shut down by its creator shortly thereafter (Pomeroy).

Online anonymity can be destructive as illustrated by the Prodigy v. Lunney case in which a user usurped another’s identity and proceeded to defame him. But it can also be seen integral to maintaining the free speech rights of the less powerful in society as well as the rights of those whose views might either be unpopular and/or potentially disturbing (without necessarily being libelous) to other individuals, groups, or institutions or businesses. The above cases dramatically underscore the critical role that ISPs are currently playing in a contemporary regulatory regime characterized largely, though not wholly, by self-regulation. The potential implications of maintaining the status quo vis-à-vis this regime as well some possible alternatives, alterations, modifications and changes are discussed below.

IV. Conclusion
A. The Ambiguous Legal Status of the ISP

The "decentralized" legacy of ARPANET has placed ISPs center stage. They are the gateways to the contemporary Internet, its traffic police, and its most "centralized" and efficient point of control and surveillance. Like it or not they have been appointed de facto -- though grudging -- arbiters of privacy and freedom of speech on the Net. As some observers have noted, they have positioned themselves as key surveillance points due in large part to the fact that systematically monitor and collect what amounts to prized data on their subscribers' action online. Yet despite their crucial position, their legal status is unclear. The FCC officially designates them as enhanced or information service providers. And statutory and case law has often -- though not always -- protected them in such a way that one might say that the ISP has come to be implicitly defined as a common carrier.

The many ways in which the ISP traverses and collapses technological boundaries and categories place it in a legal gray area. The ISP performs functions comparable to that of a common carrier, for instance the basic transmission of information. Yet it also acts in some respects like a cable provider, for example delivering access to some newsgroups but not others. In some cases, ISPs deliver access and services across cable lines and are also a cable provider. The ISP stores data in many forms and thus provides what the FCC has described as "enhanced" or "information services." It acts as a publisher of sorts, hosting web sites and newsgroups although it does not typically exercise editorial control in the same focused and directed way that a newspaper or magazine publisher does. The ISP provides access to live television and radio broadcasts as well as a vast array of videos and music and thus acts like a broadcaster are also the conduit through which direct computerized telephone and/or videophone communication occurs. The list of services provided by the ISP and the various functions as roles it performs is long and complex indeed. In a paper published in the Tulane Law Review...
which he argues that large cable providers/ISPs such as AT&T should not be required to open their lines to competing ISPs, Raymond Shih Ray Ku notes that current First Amendment doctrine determines the level of protection afforded a media entity based upon certain conceptual categories. Accordingly, under this framework must ask whether Internet service providers are more like common carriers, speakers, or gatekeepers. Unfortunately, the answer to this question is an unenlightening, yes. IS cable and otherwise, perform functions and provide services similar to telephone companies, newspapers, broadcasters, and cable television providers.

The lack of clarity with respect to the legal status of ISPs has inspired many to make comparisons to other mediums. Why, for example, aren't Internet users afforded the same statutory privacy safeguards afforded to the cable-TV subscriber and video renters, asks on EPIC attorney. And why not grant official common carrier status to ISPs, ask others. Some, troubled by the fact that private entities need not go through a formal legal process to gain information about ISP subscribers have proposed amending the ECPA so that private comp would be required to go through some kind of formalized procedure in order to obtain such and that furthermore subscribers be required to be informed before data could be acquired.

The extent of the confusing technological haze and legal maze within which ISPs are enveloped and entangled is strikingly illustrated by the fact that the FCC is considering designating Internet access by cable a "cable service." Such a decision would mean that provisions of the Cable TV Privacy Act of 1984 would be applied to Internet use over cabl but not over telephone lines. An ISP would thus face extensive restrictions on the disclosure personal information of a subscriber accessing the Net via cable, but far fewer restrictions for subscribers logging on to the Net via a modem (Pomeroy).

B. Some Proposals for Clarifying the Status of the ISP

The fuzziness with respect to the legal status of perhaps the most critically situated players in the contemporary structure of power and control on the Internet has led many to
propose a variety of changes. Some like Ku and Dmitrieva contend that the process of clarifying the status of ISPs and the privacy and free speech issues which are profoundly affected by status would be best accomplished in the courts. The conceptual complexity and specificity of many of the issues that swirl around the ISP would be best addressed on a case by case basis, they say. Dmitrieva concedes that it is a potential problem that ISPs remain outside the bounds of the First Amendment with respect to issues of censorship, but argues against sweeping constitutional or statutory changes.

In deciding the complex issues of state action as it relates to private Internet companies, courts will have to balance important countervailing interests: the First Amendment interests of Internet users and free speech rights of Internet providers; the proprietary interests of Internet companies and the democratic ideals of the U.S. society. (22)

Citing the inconsistencies in the Maxwell and Hambrick rulings, Mark Elmore in a brief published in the Texas Tech Law Review asserts that the courts are not equipped with sufficient technological knowledge to decide important First and Fourth Amendment Internet issues themselves:

Judges do not possess the technical expertise and knowledge to make the necessary determinations in deciding whether an individual has a reasonable expectation of privacy in a particular Internet related activity. If changes are not made at the legislative level, courts will continue to make individual determinations that could result in a lack of uniformity in protection.

Elmore, whose brief makes an argument that the ECPA is so vague as to offer no real legal basis upon which to regulate Carnivore, proposes amendments to the ECPA such that the definition of "electronic communications" would list e-mail specifically, and that furthermore the ECPA be defined to include all parts of an e-mail, including header, address, and body packets. Joseph Kampherstein in a Temple and Environmental Law & Technology Journal article that focuses on Carnivore also contends that changes in statutory law are needed to clarify and bolster privacy rights with respect to e-mail:
The Fourth Amendment was designed with the thought that one’s “papers and effects” were among the most desirous of protection from the intrusions of government. Congress should recognize that storage of e-mail at an ISP is most closely analogous to storage of postal mail in a post office box until retrieval and reading, and therefore offer a higher degree of protection to stored e-mail. The definition of “interception” should include opening or deletion of e-mail prior to opening by the recipient. This definition is already gaining judicial acceptance, and should be recognized and clarified through legislation.

Others contend the current regulatory scheme is adequate. In an article in *The Internet Newsletter* explaining the basic provisions of the ECPA,9 Beth Maloney, an attorney for a Massachusetts ISP, seeks to defuse fears that ISPs are too easily and quickly yielding to government surveillance requests. “Given the prevailing anxiety concerning lack of privacy on the Internet, users should be reassured of the fact that their ISPs are making reasonable efforts to ensure that a subscriber’s privacy rights are being protected,” she writes. “The provisions of ECPA, grounded in Fourth Amendment jurisprudence, grant ISPs the legal and constitutional backbone with which to protect subscriber rights.”

Some Internet scholars and writers have called for a market regulatory scheme in which a range of specialized ISPs would offer subscribers varying “levels” of access to the Net, with some ISPs screening out more content than others and consumers signing up with whichever ISP’s censorship approach most suited their own normative standards (Taylor). Still others issued calls to officially designate ISPs as common carriers. “As the provider of the channel and network for communication, the ISP should not be held liable for content made available through its infrastructure. We do not, after all, prosecute the telephone operator when people discuss illegal or immoral subjects over the phone. It would be all but impossible for an ISP to regulate every use of its network cost-effectively,” contends Computer Weekly writer Simon Preston. Others have called for a combination of regulatory schemes under which ISPs would be designated as common carriers and a system of digital IDs and zoning of the Net—PICS, or...
Platform for Internet Content Selection is most frequently mentioned — much like that described by Lawrence Lessig\textsuperscript{10} would be instituted.

C. The Future Status of the ISP and Privacy and Free Speech on the Net

Nothing less than the future of basic privacy and free speech rights is at stake in the struggle over the legal status of ISPs, their rights and the rights of their subscribers, and the role in surveillance and content control of the Internet. The struggle’s players and stakeholders are many. They include ISPs, businesses, law enforcement agencies, government, intelligence agencies, activists, and human rights and civil liberties advocates. If the following assessment of the future by ISP-Planet Managing Editor Patricia Fusco is at all representative, ISPs are clearly anxious about the future:

As legislators rush to embrace the residual benefits of e-commerce while strangling gateways and exchanges with filters, encryption restrictions, and content banishment Internet service providers and Web content hosts must prepare for serious government attempts to eradicate freedom of expression on the Internet. If service providers don’t stand and act now, what was once referred to as the ‘Information Superhighway’ enriched by a free flow of Internet content and unrestricted access, may have less content than public access television, with ISPs and WPPs acting as the ‘Net Police’ of the w

Although it is not possible here to develop a detailed regulatory framework that would once for all clarify the status and role of the ISP, simply keeping the current regime of self-regulation intact is highly problematic. The kind of self-regulation in which ISPs for the most part now engage could, as some predict, increasingly become dictated by outside forces and thus instill kind of anxiety driven self-censorship that begins to threaten free expression on the Net. Self-regulation practiced under pressure from outside forces and the fear of potentially debilitating libel suits could also threaten the privacy of subscribers whose identities might be revealed easily — to both government and private entities — by anxious ISPs. And anxious subscribers could ultimately mean “chilled speech.” Finally, with the lurking specter of concentration of ownership, the problems with a self-regulatory regime mentioned here could well be intensi-
Given trends in other media, it is not far-fetched to predict that the future will bring fewer and fewer ISPs who will act as the gateways, flow directors and monitors for more and more subscribers. Fewer and larger ISPs could lead to a homogenizing effect in which those ISPs, pressured by dominant mainstream interests, might become increasingly likely to censor "unpopular" ideas and points of view and/or limit access to those points of view. Although there are many important differences between newspaper publishers and ISPs, larger newspapers more readers typically deliver a much more homogenized and sanitized news product than smaller publications from both the right and left wings of the political spectrum. They do so arguably because it is in their economic interest to please the most readers and offend the few. Certainly it is not out of the realm of possibility that it could come to be in the economic interest of a few large ISPs to chart a similarly safe course with respect to "fringe" ideas posted on newsgroups and "radical" points of view expressed in "controversial" web sites. In a market of extreme concentration of ownership (by no means an assured development), it is conceivable subscribers could have few if any choices outside of the larger, politically and ideologically sanitized ISPs.

If keeping the current regulatory regime in place is problematic, so too is relying exclusively upon case law to determine the future status of the ISP and the multiple privacy and freedom of speech issues that swirl around it. A combination of carefully considered changes in statutory law and subsequent clarifications made by way of case law may be best approach matter what regulatory scheme is pursued it is imperative that it seek to vigorously protect privacy and free speech rights of ISP subscribers. "Personal privacy," writes Stefik, "is abut freedom from surveillance, freedom from intrusion, and security for our personal records. All these themes of privacy concern preventing other people from monitoring our activities" (199). And Bowden and Akdeniz assert that,
Security authorities argue that flexible options for large-scale surveillance are needed intelligence-led operations to counter organised crime, or proliferation of weapons of mass destruction. But if the design of the new communications infrastructure is predicated on an absolute capability to counter such threats, the resulting apparatus indistinguishable from that required to anticipate, subvert, and neutralise political di
(101).

In chiseling out a workable regulatory framework which adequately addresses the many complexities inherent to the ISP and its critical position with respect to issues of privacy and speech, we must ensure that the right to dissent so fundamental to modern democracy does not get quashed in the process. We must be careful not to give in to a dominant view in which a expanding regime of electronic surveillance increasingly comes to be justified by the commonsense notion "I didn’t do anything wrong, why should I be worried?" or, "If you’re anxious about being watched by your ISP, what is it that you have to hide?"

William G. Staples in his book *Everyday Surveillance: Vigilance and Visibility in Postmodern Life* contends that in contemporary American society, "Surveillance and discipline have become oddly democratic; everyone is watched, and no one is trusted" (4). If Staples is right -- and there are strong indications that he is -- it would seem that many if not most Americans have given up what could be reasonably called a "reasonable expectation of privacy." Kampherstein defines a "reasonable expectation of privacy" first hammered out in the defining *Katz v. the United States* Supreme Court case as being contingent upon a "twofold" test. "First, the person must exhibit an actual expectation of privacy, that is, the taking of demonstrative action consistent with an expectation of privacy. Second, it must be shown that society accepts that expectation as reasonable." The second test is of profound significance. For if larger so acquiesces to an increasingly penetrating regime of surveillance and control, a regime that is increasingly manifesting itself on the Internet at the level of the ISP, the threshold for a "reasonable expectation of privacy" will drop accordingly. Such a drop could have dramatic far-reaching repercussions for those whose actions, ideas, politics and ideologies fall outsid-
bounds of the mainstream in what Alexis de Toqueville were he alive today might well call
cyberspatial expansion of an ever deepening and increasingly sweeping "tyranny of the
majority."

---

**Endnotes**

1 In March of 2001, for example, hackers hacked into the web site of Hamas, a radical Islamic group
placed a link on the page that automatically redirected users to a pornographic site as soon as the
page was loaded. Hamas accused the Israeli intelligence operatives of carrying out the cyber attack
one claimed responsibility for the attack ("Hackers Put Pornography on Hamas Web Site").

2 DNS “structures the assignment of names on the network and converts those names to their uni
addresses” (King et al. 18). In other words it ensures that specific information requests sent across the
Network via a Transfer Control Protocol command (TCP) will result in the right information being:

3 Germany in 1997 passed into law the Information and Communication Services Act (ISCA). The
subjects ISPs to criminal prosecution for knowingly acting as a conduit for illegal content that it
technically possible to halt in transmission. The ISCA also requires that ISP offices have bureauacr
"Youth Protection Officers,” to troll the Internet for objectionable material. In addition, it mak
crime to disseminate or make accessible materials deemed harmful to children (McGuire).

4 "The set of full routes contained in the core routers' tables defines the reach of the Internet. Each
associated with an IP address (or net ID) stored in the core routers' tables can communicate with al
devices associated with IP addresses at those tables. A device that is not associated with any IP add
the full routing table will be invisible to a large portion of the Internet. Given the rapid expansion
Internet, maintenance of the core routing tables is a critical and demanding task for the core IS
(Milgrom et al 18; authors' emphasis)

5 According to a detailed *Information Week* account of the incident published an April 2001 issu
December 1999, U.S. marshals served officials of EarthLink with a court order to install a commer
available device called "EtherPeek," which would be connected to the ISP's Pasadena, Calif., netw
to let the government monitor electronic messages on the system. Citing concerns that the device be capable of snooping in on all subscribers' data, Earthlink sought and received permission to put it customized surveillance software on the network. However the government insisted on installing it device. EarthLink filed a motion to quash the original court order. During this legal proceeding government revealed that it planned to use a new, proprietary device by the name of Carnivore. Ca was incompatible with EarthLink's operating system software and EarthLink crashed. *Information*
reports that, "Exactly when it crashed and for how long and the extent of the damage, if any, th
caused by Carnivore or whether customer E-mails were delayed or lost is unclear because EarthLi
the FBI refuse to discuss the episode. The magistrate's order is sealed from public view, and Earth
officials won't discuss it.” An Earthlink spokesperson is quoted by *Information Week* as saying, "W
a business relationship with the FBI now. We have our own method to give them what they wai
(Kahaner).

6 Two copyright hunting firms, MediaForce and Copyright.net (which is doing anonymous work f
of the "big five record labels) have created automated systems which search file-swapping netwo
their clients' work. Once the music is found, the IP address of the computer on which files are sit identified. The companies then cross-reference the information with the ISP that owns the IP address and send a letter that documents which files are being shared and which demands that the subscriber stopped.

7 EPIC and the ACLU charged that the review, which was released on Nov. 21, 2000, was not indep of government influence and that the DOJ report had been "sanitized." The review found that Carnivore program works pretty much the way the FBI said and that it did not overcollect extraneous from untargeted subjects, as privacy advocates feared. However, the reviewers did find that it fa adequately track individual accountability for all Carnivore actions and they recommended that it establish additional safeguards when using the system ("Institute's Report on Carnivore Causes U Among Critics").

8 Dmitrieva finds the case law record mixed with respect to the application of the state action doctrine. Shopping malls, noting that in some cases state supreme courts have allowed demonstrators and pick access to malls in California and New Jersey but not in others (Minnesota). In examining the case record with respect to news providers, she finds that "as a rule, courts are reluctant to find state ac cases involving First Amendment challenges to conduct of private news providers. Even state media, such as public television stations, enjoy a large degree of editorial discretion in defining content of their programming" (15). With respect to telephone companies, Dmitrieva finds that they adopt content-based regulations on speech as long as they do it as a matter of independent business policy" (16). But she also notes that if states exercise pressure on phone companies to pursue practices and polices the "courts could find an element of state action" (17).

9 Maloney explains that "According to § 2703 (of the ECPA), the requirements for government ac information in the possession of an ISP vary depending upon the classification of the information sought. Personal information is broken down into three classifications: (a) Contents of Electronic Communications in Electronic Storage; (b) Contents of Electronic Communications in a Remote Computing Service; (c) Records Concerning Electronic Communication Service or Remote Computing Service. Content, in keeping with tradition, is allocated the highest degree of protection from governmental intrusion. Government officials are required to obtain a warrant to gain access to communications in electronic storage for less than 180 days. The protocol is slightly relaxed if the content of the communication has been in storage for more than 180 days. In that case, if the subscriber is notified through a subpoena or court order, they have the authority to demand disclosure of the content information from the subscriber's ISP. For the contents of electronic communications in a remote computing service, the same rules as for communications in electronic storage for over 180 days."

10 In his seminal book *Code and Other Laws of Cyberspace* Lessig proposes a code-driven archit which deploys digital certificate technologies and zoning as the best way to strike a balance bet freedom and constraint and to realizing the individual and collective accountability he views as nec to achieve freedom on the Internet. Under such an architecture, users would need digital ID's to v the "hallways" of the Internet, but their anonymity would be protected by "trusted third parties' could certify facts about them using "dual" or "asymmetric encryption". User's freedom of mov across the Net would be conditioned based on customized credentials held by the users. So, for exar user with a child's ID would not hold the necessary credentials to access parts of the Net that has electronically zoned to keep them out. As a sort of driver's license for the Net, the digital certificate to users could also be used to hold individuals accountable for unlawful actions.
Works Cited


