Borders in Cyberspace

Information Policy and the Global Information Infrastructure

edited by Brian Kahin and Charles Nesson

A Publication of the Harvard Information Infrastructure Project

The MIT Press, Cambridge, Massachusetts, and London, England

The Internet as a Source of Regulatory Arbitrage

A. Michael Froomkin

The Modern Hydra?

Hydra was a mythical beast with many heads, one of which was immortal.[1] Every time one of its heads was cut off it grew two more. To regulators, the Internet may seem like a modern Hydra. Almost every attempt to block access to material on the Internet, indeed anything short of an extraordinarily restrictive access policy, can be circumvented easily. Hydras can be killed by heroic measures: according to Greek mythology, Hercules ultimately destroyed Hydra by cauterizing its stumps and severing the immortal head from its body. The Internet, too, could be killed, or a nation could choose to allow access on a restricted basis. Yet, the more a nation pursues a restrictive Internet policy, the less value it will derive from the network and the more it risks being left out of the information revolution.

Three technologies underlie the Internet's resistance to control. First, the Internet is a *packet switching network*, which makes it difficult for anyone, even a government, to block or monitor information flows originating from large numbers of users. Second, users have access to powerful military-grade cryptography that can, if used properly, make messages unreadable to anyone but the intended recipient. Third, and resulting from the first two, users of the Internet have access to powerful anonymizing tools. Together, these three technologies mean that anonymous communication is within reach of anyone with access to a personal computer and a link to the Internet unless a government practices very strict access control, devotes vast resources to monitoring, or can persuade its

population (whether by liability rules or criminal law) to avoid using these tools.

The vision of the Internet as a threat may in any case be flawed. Hydra was a dangerous monster; the Internet, despite the real difficulties it will pose for certain types of regulation, may be predominantly benign.

Packet Switching

The Internet is not a thing; it is the interconnection of many things—the (potential) interconnection between any of millions of computers located around the world. Each of these computers is independently managed by persons who have chosen to adhere to common communications standards, particularly a fundamental standard known as TCP/IP,[2] which makes it practical for computers adhering to the standard to share data even if they are far apart and have no direct line of communication. TCP/IP is the fundamental communication standard on which the Internet has relied: "TCP" stands for Transmission Control Protocol, while "IP" stands for Internet Protocol. There is no single program one uses to gain access to the Internet; instead there are a plethora of programs that adhere to these Internet Protocols. A computer connected to the Internet may have any number of users, all or none of whom may have any of widely varying levels of access to other computers in the network.[3]

The TCP/IP standard makes the Internet possible. Its most important feature is that it defines a packet switching network, a method by which data can be broken up into standardized packets which are then routed to their destinations via an indeterminate number of intermediaries.[4] Under TCP/IP, as each intermediary receives data intended for a party further away, the data are forwarded along whatever route is most convenient at the nanosecond the data arrives. It is as if rather than telephoning a friend one were to tape record a message, cut it up into equal pieces, and hand the pieces to people heading in the general direction of the intended recipient. Each time a person carrying tape would meet anyone going in the right direction, he or she would hand over as many pieces of tape as the recipient could comfortably carry. Eventually the message would get where it needed to go.

Neither sender nor receiver need know or care about the route that their data take and there is no particular reason to expect that data will follow the same route twice. (More importantly from a technical standpoint, the computers in the network can all communicate without knowing anything about the network technology carrying their messages.) Indeed, it is likely that multiple packets originating from a single long data stream will use more than one route to reach the far destination where they will be reassembled. This decentralized, anarchic method of sending information appealed to the Internet's early sponsor, the Defense Department, which was intrigued by a communications network that could continue to function even if a major catastrophe (such as a nuclear war) destroyed a large fraction of the system.[5] The Internet can use dedicated lines or messages can travel over ordinary telephone connections. This built-in resilience is the primary reason that any effort to censor the Internet is likely to fail.

The widespread use of TCP/IP enables the functions that have come to be identified with the Internet, notably: electronic mail (e-mail), Usenet, the World Wide Web, file transfer protocol (FTP), Gopher, Wide Area Information Server (WAIS), Internet Relay Chat (IRC), Multiple User Dungeons/Domains (MUDs), and MUD Object Oriented (MOOs), to name only the most commonly used functions. A user who has access to one of these functions does not necessarily have access to others because the user's level of access is determined by the type of computer used, the capacity of the Internet connection, the cost of access, the software used, and the policy of the person or organization operating that computer. Some national governments impose additional constraints on Internet connectivity. Today it is still possible for a government to restrict access to the Internet; once a person is connected, however, it is currently beyond the power of any government to limit what is accessible via the Internet.

Decentralized Standard Setting

The Internet standard-setting process is also decentralized. Standards are set by an international unincorporated nongovernmental organization known as the Internet Engineering Task Force (IETF). The IETF allows unlimited grassroots participation and

operates under a relatively large, open agenda. The IETF has no general membership; instead, it is made up primarily of volunteers, many of whom attend the organization's triennial meetings. Meetings are open to all; similarly, anyone can join the e-mail mailing list in which potential standards are discussed.[6] Although the IETF plays a role in the selection of other groups that help define the basic Internet protocols, the IETF is not part of or subject to those groups. Indeed, it is not entirely clear to the membership who if anyone "owns" the IETF or for that matter who is liable if it is sued.[7] An amorphous body of this sort may be difficult to sue; it is even harder to control.

The IETF has a complex relationship with three more traditionally bureaucratic structures that ensure its continued existence and cohesion: the Internet Society (ISOC), the Internet Architecture Board (IAB), and the IETF Secretariat. The ISOC was founded in January 1992 as an independent, international "professional society that is concerned with the growth and evolution of the worldwide Internet, with the way in which the Internet is and can be used, and with the social, political, and technical issues which arise as a result."[8] The ISOC Board of Trustees must approve all nominations to the IAB. The IAB, formerly the Internet Activities Board, is a technical advisory sub-group of the ISOC responsible for providing oversight of the architecture of the Internet and its protocols. The IAB enjoys a veto over standards proposed by the IETF. Randomly selected members of the IETF control the nominations for the IAB, but the IETF is not formally part of or subject to the IAB. The IAB also retains considerable control over the assignments given to the almost ad hoc task forces that do most of the IETF's work. The IETF Secretariat organizes the triennial meetings and provides institutional continuity between meetings, e.g., by maintaining a World Wide Web site. The Secretariat is administered by the Corporation for National Research Initiatives, with funding from U.S. government agencies and the ISOC. The Secretariat also maintains the on-line Internet Repository, a set of IETF documents.[9]

Growing Uses and User Base

In 1983 there were perhaps 200 computers on the ARPANET, the precursor of the Internet. As of January 1993, there were more than 1.3

million computers with a regular connection to the system. In January 1996 there were about 9.4 million Internet *hosts*, computers regularly connected to the Internet,[10] with a substantial fraction, but probably less than half, located outside the United States. Each of these computers is likely to have at least one user, and some have many more. In 1983 only a handful of networks existed;[11] a 1993 estimate suggested that the Internet connected to approximately 50,000 networks and 30 million users, although that estimate seems high. Access has been doubling annually.[12] Current estimates of connectivity vary; one study suggests 40 million users worldwide.[13] The most careful recent study of U.S. usage found 28.8 million adults with potential or actual access but only 16.4 million people 16 years and over who actually used the Internet in the previous three months.[14] Whatever the actual numbers, there seems to be a consensus that usage is growing exponentially and that non-U.S. users will soon reach 50% of the total. At this rate of growth, the Internet cannot help but penetrate deeply into the general population of industrialized countries.

The two most successful Internet applications have been electronic mail—an estimated 25 billion e-mail messages were exchanged in 1995[15]—and the World Wide Web. The Web is an Internet client-server hypertext-distributed information retrieval system.[16] Within two years of its introduction to the public in 1991, the amount of Web traffic traversing the NSFNET Internet backbone reached 75 gigabytes per month, or one percent of the total. By July 1994 Web traffic was one terrabyte (one million megabytes) per month,[17] and a recent estimate puts it at 17.6% of the total Internet traffic.[18] Web browsing programs such as Netscape or Explorer allow the user to navigate the Web in hypertext. Hypertext links inserted by document authors refer the reader to other documents using Uniform Resource Locators (URLs). A mouse click on a link refers the user to remote documents, images, sounds, or even movies that have been made Internet-accessible. A Web browser can retrieve data via FTP, Gopher, Telnet or news, as well as via the http protocol used to transfer hypertext documents.[19]

How the Internet Enables Anonymous Communication

Communicative anonymity allows users to engage in political speech without fear of retribution, to engage in whistle blowing

while greatly reducing the risk of detection, and to seek advice about embarrassing personal problems without fear of discovery. It also has costs, since it vastly reduces the chances of identifying the authors of libel, hate speech, and other undesirable communications.

Thanks in large part to the easy availability of powerful cryptographic tools, the Internet provides the ability to send anonymous electronic messages at will. Cryptography alone, however, is not enough. Full communicative privacy and anonymity requires the services of third parties such as *remailer operators*, who volunteer to operate anonymous *remailer* programs. As described in more detail below, the anonymously mailed e-mail cannot, when properly formatted by the sender for transmittal via these intermediaries, be traced back to its originator. In addition, by using remailers two or more persons can communicate without knowing each other's identity while preserving the untraceable nature of their communications.

It is useful to distinguish between four types of communication in which the sender's physical (or "real") identity is at least partly hidden: *traceable anonymity, untraceable anonymity, untraceable pseudonymity,* and *traceable pseudonymity.* These categories allow one to disentangle concepts that are otherwise conflated: whether and how an author identifies herself as opposed to whether and how the real identity of the author can be determined by others.[20] By untraceable anonymity and pseudonymity I mean a communication transmitted in a manner that provides no information that would aid in identifying the author. For example, if Alice drops an unsigned leaflet that is free of fingerprints on Bob's doorstep in the dead of night when no one is looking, her leaflet might be "untraceably anonymous" if the paper and typeface were sufficiently generic.

The traditional anonymous leaflet required a printing and distribution strategy that avoided linking the leaflet with the author. If the leaflet risked attracting the attention of someone armed with modern forensic techniques, great pains were required to avoid identifying marks such as distinctive paper or fingerprints. In contrast, on the Internet communications are all digital; the only identifying marks they carry are information inserted by the sender, the sender's software, or by any intermediaries who may have relayed the message while it was in transit. For example, an e-mail

message ordinarily arrives with the sender's return address and routing information describing the path it took to get from sender to receiver; were it not for that information, or perhaps for internal clues in the message itself ("Hi Mom!"), there would be nothing about the message to disclose the sender's identity.

Enter the anonymous remailer. A remailer receives and automatically forwards communications in a manner that disguises the identity of the original sender. If Alice, the original sender, uses a little care and sends a message via a series of remailers that take advantage of cryptographic tools, the remailer operators need not be known to be trustworthy. Instead, as shown below, Alice's anonymity is protected against anything but the most determined eavesdropping and message-tracing effort so long as any one operator in the chain of intermediaries does not conspire with all the other intermediaries to learn the sender's identity. The more remailers in the chain, however, the longer it may take the message to get to its destination and the greater the chance that an operator in the chain will fail to pass the message on down the line.[21]

Remailers vary, but all serious remailing programs share the common feature that they delete all identifying information about incoming e-mails, substituting a predefined header identifying the remailer as the sender or using a cute tag such as nobody@nowhere.[22] By employing easily automated cryptographic precautions widely available on the Internet and routing a message through a series of remailers, Alice can ensure three outcomes conducive to high security anonymity: (1) None of the remailer operators (except possibly the last in the chain) will be able to read the text of the message because it has been multiply encrypted in a fashion that requires the participation of each operator in turn before the message can be read. (2) Neither Bob, the recipient, nor any remailer operator in the chain (other than the first in the chain) can identify Alice without the cooperation of every prior remailer's operator. (3) It is therefore impossible for the Bob to connect Alice to the text unless every single remailer in the chain both keeps a log of its message traffic and is willing to share this information with the recipient (or is compelled to do so by a court or other authority). Since some remailer operators refuse to keep logs as a matter of principle, there is a good chance that the necessary information does not exist. Even if logs exist, it could be prohibitively expensive

for a private litigant to compel all of the operators to divulge their logs because the user can select remailers located in different countries, exposing the would-be plaintiff to the expense of hiring foreign legal counsel and possibly to language difficulties. Similarly, criminal prosecutions may run into difficulties because many legal systems require that an act be an offense in both jurisdictions before allowing a prosecution, or in some cases even discovery, to proceed.

Any electronic communication, even live two-way "chat" communication, can theoretically be made anonymous.[23] In current practice, anonymous remailer technology applies only to e-mail and hence is used for communication between individuals, for mailing lists, and for newsgroup discussions. Although e-mail remailer technology may not yet be as user-friendly as it could be, it is available to anyone who knows where to look—and can even be found on an easy to use World Wide Web page.[24] Anonymous World Wide Web proxies are currently being tested.

At the simplest level, encryption ensures that the first remailer operator cannot read the message and effortlessly connect Alice to Bob and/or the contents. But encryption also has a far more important and subtle role to play. Suppose that Alice decides to route her anonymous message via Ted, Ursula, and Victor, each of whom operates a remailer program and each of whom has published a public key in a public-key encryption system such as PGP.[25] Alice wants to ensure that no member of the chain knows the full path of the message; anyone who knew the full path would be able to identify Alice from the message Bob will receive. On the other hand, each member of the chain will necessarily know the identity of the immediately previous remailer from which the message came and of course the identity of the next remailer to which the message will be sent.

Alice thus wants Ted, the first member of the chain, to program his remailer to remove all information linking her to the message; she is particularly anxious that Ted not be able to read her message since he is the one party in the chain who will know that Alice sent it. Alice also wants Ted to know only that the message should go to Ursula and to remain ignorant of the message's route thereafter. Alice wants Ursula, the second member of the chain, to know only

that the message came from Ted and should go to Victor (and to remove the information linking Ted to the message as extra insurance); Victor should know only that it came from Ursula and should go to Bob, although by the time the message reaches Victor, Alice may not care as much whether Victor can read the message since her identity has been well camouflaged.

Alice achieves these objectives by multiply encrypting her message, in layers, using Ted's, Ursula's, and Victor's public keys. As each remailer program receives the message, it discards the headers identifying the e-mail's origins and then decrypts the message with a unique private key, revealing the next address but no more. If one thinks of each layer of encryption as an envelope with an unencrypted address on it, one can visualize the process as the successive opening of envelopes. Thus Alice sends a message to Ted which reads:

To: Ted
Message encrypted with Ted's private key

Please forward to: Ursula
Message encrypted with Ursula's public key

Please forward to: Victor
Message encrypted with Victor's public key

Please forward to: Bob

Text of anonymous message.

Ideally, this is encrypted with Bob's public key, but even if it is plaintext, Victor should be unable to connect it to Alice as long as Alice remembers not to sign her name.

Chaining the message through Ted, Ursula, and Victor means that no remailer operator alone can connect Alice either to the text of the message or to Bob. Of course, if Ted, Ursula and Victor are in a cabal, or all in the same jurisdiction and keep logs that could be the subject of a subpoena, Alice may find that Bob is able to learn her identity. All it takes to preserve Alice's anonymity, however, is a single remailer in the chain that is not a member of the cabal and either erases her logs or is outside the jurisdiction. In theory, there is no limit to the number of remailers in the chain; Alice can, if she wishes, loop the message through some remailers more than once to throw off anyone attempting *traffic analysis*, which is the study of the sources and recipients of messages, including messages that the eavesdropper cannot understand.[26]

Nothing is foolproof, however. If Alice has the bad luck to use only compromised remailers whose operators are willing to club together to reveal her identity, she is out of luck. However, if Alice uses both encryption and chaining and one member of the chain refuses to cooperate in the effort to unmask her, Bob should not be able to trace the message's path from himself back to Alice. An extraordinarily determined eavesdropper, able to track messages going in and out of multiple remailers over a period of time (perhaps using wiretaps on telephone lines), might be able to conduct traffic analysis and correlate messages leaving one remailer with those arriving at another. To foil this level of surveillance, which has nothing to do with the bad faith of the remailer operators, requires even more exotic techniques including introducing random delays into the remailing process, having the remailers alter the size of messages, and ensuring that they are not remailed in the order they are received.[27]

The supply of remailer operators is the major potential constraint on Internet anonymity. Remailer programs are currently operated by a relatively small number of volunteers located in a few countries; at present they receive no compensation for this service, and in the absence of anonymous electronic cash or the equivalent it is difficult to see how an electronic payment system could be constructed that would not risk undermining the very anonymity the remailers are designed to protect.

The remailer operator's problem is a simple one. No operator can control the content of the messages that flow through the

remailer. Furthermore, the last remailer operator in a chain has no reliable way of concealing the identity of the sender's machine from the message's ultimate recipient. Suppose, to return to the example above, Alice wants to send an anonymous death threat to Bob via remailers operated by Ted, Ursula, and Victor. If Victor does nothing to mask his e-mail address, Bob will know he was the last to remail the message. Victor can make any attempt to identify him more difficult by forging his e-mail address in the message to Bob, but Victor cannot be certain that this will work. Indeed, he can be almost certain that over time it will fail.

To understand why this is so requires some background in how an ordinary e-mail message is transmitted from Alice's machine to Bob's via the Internet. As we have seen, ordinarily the two computers do not communicate directly. Instead Alice's machine sends the message to a machine that it hopes is in Bob's general direction, and the message passes from machine to machine until it finds one that is in regular communication with Bob's. Each machine that handles the message appends "path" information to the e-mail that identifies it as having taken part in the communication. The final recipient receives the entire set of path data along with the text of the message, but most commercial e-mail packages are designed to avoid displaying this path information to the reader unless she asks for it.

Victor can instruct his computer to lie about its identity, and indeed can forge information suggesting that the message originated elsewhere far away, but he has no way to persuade the machine to which he sends the message to cooperate. As a result, it is possible for a sufficiently motivated Internet detective to identify the first machine to which Victor sent the message, especially if she has several messages to work with.[28] If the machine that communicated with Victor keeps records of its e-mail handling, or if its operator can be persuaded to do start doing so, the Internet detective can identify Victor's machine, and perhaps even Victor, as the source of the remailed message.

Ordinarily, however, no detective work is required to identify the last remailer in a chain because remailer operators do not attempt to hide their identity. The last remailer is thus exposed to the wrath of an unhappy recipient. Additionally, an identifiable person is a potential target for regulation. If, for example, the remailer opera-

tors were made strictly liable for the content of messages that passed through their hands, even though they were unable to learn the content of those encrypted messages, most reasonable people probably would find running a remailer to be an unacceptable risk if they resided in a jurisdiction capable of enforcing such a rule.

Some jurisdictions may choose to make life difficult for remailers. Indeed, in the eyes of some, remailers are a public health hazard on the order of AIDS and other virulent diseases. These writers suggest that remailers enable "information terrorism," although they do not define this term with any precision.[29] Already, they suggest, remailers are "frequently used by the Russian (ex-KGB) criminal element" and favored by unspecified parties for engaging the services of unspecified "cybercriminals."[30] However wild, untestable, and indeed irrefutable, these accusations may be, they contain one grain of truth: remailers do allow users to avoid being held responsible for the contents of the messages they send. In theory at least—I am unaware of any documented examples in practice—a third party could set up shop as an honest broker between an anonymous client and an anonymous criminal and plausibly plead ignorance as to the nature of the transaction.

Remailer operators already have come under various forms of attack, most recently the legal proceedings instigated by officials of the Church of Scientology who sought to identify the person they allege used remailers to disseminate copyrighted and secret Church teachings. At some point, if the number of remailers is small, it becomes technically (if not necessarily politically or legally) feasible for the authorities to conduct traffic analysis on all the remaining remailers and make deductions about who sent what to whom. In the absence of a compensation mechanism or a jurisdiction capable of offering a safe haven for remailers, the cornerstone of Internet anonymity currently relies entirely on the charity of strangers.

Why Censorship Is Difficult

In most countries, all that is required for access to the Internet is either a home computer with access to an Internet service provider (ISP) or an account on a computer network that has Internet

access, such as those found in most universities. Short of cutting off international telephone service or concluding an international agreement with all industrialized countries to discontinue telephone service with foreign countries that harbor remailers, there is little that governments can do keep out messages from any other country, or indeed to keep citizens from sending messages wherever they like.

Content control today is frequently primitive or nonexistent. For example, *Penthouse* magazine's World Wide Web site announces that the Web site is "not available" in Ecuador, Egypt, Fiji, Formosa, India, Japan, Kenya, Korea, Malaysia, Malta, Mexico, Nigeria, Okinawa, Pakistan, the Philippines, Saudia Arabia, Singapore, South Africa, Spain, St. Lucia, Thailand, Trinidad, Turkey, the United Kingdom, and Venezuela because these nations "prohibit adult material."[31] Nevertheless, I am reliably informed that the materials on this Web site are accessible from a domain in the United Kingdom with an address ending in ".uk."

If the government of Ruritania is intent on preventing communication with Great Britain, Ruritania might attempt to require that Ruritanian ISPs refuse to accept messages from computers whose domain name identifies them as British. British domain names frequently end with ".uk," and Ruritanian routers might be required to return all messages from those domains. Even if technically feasible, such a strategy is unlikely to succeed. First, there are generic domain names such as ".com," ".org," and ".net" that do not identify the country of origin. Second, unless Ruritania has currency and other controls, there is nothing to stop a Ruritanian user from establishing an account in the U.S. and telnetting to it to access British data. (Even currency controls may not prevent users from establishing foreign Internet accounts since some accounts, on so-called "freenets," are free to the public.) Third, short of a robust international convention, there is no way that Ruritania can prevent people outside Britain from running remailers that "launder" messages from Britain and present Ruritanian computers with acceptable domain names. In short, any effort to censor the Internet organized at the national level (or below) is likely to fail.[32] As John Gilmore put it, "the Net interprets censorship as damage and routes around it."[33] Of course, nothing prevents individual

users or system operators from blocking the direct receipt of messages from unwanted sources. Users, however, will not find it difficult to circumvent these restrictions for e-mail, although it might be technically feasible to eliminate anonymous postings from Usenet, a distributed bulletin board system, as long as the number of remailers remains small.[34]

Regulatory Arbitrage . . . and Its Limits

The Internet is a multinational phenomenon. Indeed, as long as they share a common language and a reasonably rapid connection, users of the Internet will frequently be indifferent to the physical location of those with whom they communicate. Location matters little for speech; it may matter more for commerce when parties to a transaction are concerned about redress for a transaction that goes badly. To the extent that transactions are immediate (e.g., exchanges of information) or that suitable reputations, performance bonds, or other third-party guarantees enable longer-term relationships,[35] the multinational nature of the Internet makes it possible for users to engage in *regulatory arbitrage*—to choose to evade disliked domestic regulations by communicating/transacting under regulatory regimes with different rules. Sometimes this will mean gravitating to jurisdictions with more lenient rules, or perhaps no rules at all; sometimes it will mean choosing more stringent foreign regimes (e.g., those with strong consumer protection laws) when stricter rules are more congenial.

Censorship Suffers

Simple communication—free speech—is the strongest example of regulatory arbitrage. Other countries that lack a First Amendment may choose solutions to the perceived dangers of anonymous communication that are more or less restrictive than those suggested by U.S. law, which itself remains unclear in important respects. Remarkably, however, the technology for sending e-mail messages anonymously is already in use both here and abroad; the whole world can now enjoy (or suffer) the fruits of anonymous remailers located anywhere. The constitutional status of anony-

mous electronic speech remains important: if the U.S. will not or constitutionally cannot ban anonymous remailers, then the U.S.'s Internet connectivity ensures that they will be available for the entire Internet to use. Even if the U.S. attempts to ban anonymous remailers, and even if the Constitution is interpreted as allowing this, U.S. law may not be determinative because, as it now stands, the Internet as a whole is not easily amenable to any nation's control. While it is probably within the physical power of the U.S. government to prosecute Internet remailers based in U.S. territory, it is difficult to see how in practice the government could prevent U.S. residents from using remailers located abroad, although it could certainly raise the costs of getting caught.[36]

U.S. law currently imposes few if any legal restrictions on anonymous remailing. U.S. rules can thus be viewed as a baseline; any country with a more restrictive approach to anonymity can expect to see it undermined by U.S. rules unless it is willing and able to cut itself off from the Internet entirely. Similarly, should the U.S.'s rules change to restrict anonymity, as they might some day, these new rules will themselves be undermined by persons in any another country with more than minimal Internet connectivity and a legal regime more congenial to anonymous communication. (For example, the Canadian Copyright Act guarantees the right of an author to write under a pseudonym.[37]) The proponents of measures to regulate Internet speech and eliminate Internet anonymity are thus likely to find themselves in the position of the counselors to King Canute. Indeed, to the extent that countries with good Internet connectivity such as the Netherlands and Finland already have more permissive rules, those rules effectively undercut the U.S.'s ability to enforce what rules it has.

Once it allows its citizens to connect freely to the Internet, the ability of a government to control the flow of information in a meaningful way is greatly reduced. Anyone with access to e-mail, USENET, or the World Wide Web can receive electronic samizdats at will; anyone with access to e-mail or an anonymous Web page can send out information in a manner that is almost impossible to track. Nevertheless, as long as the Internet remains an elite medium rather than a mass medium, government controls on mass communication will retain some effectiveness.

Asian Examples of the Practical Limits to Censorship

The difficulty that governments have in reigning in free speech on the Internet or in living with its consequences is particularly visible in the uneasy relationship that several Asian governments have with the Internet. Only North Korea and Myanmar have chosen to remain completely aloof from it.[38] The Vietnamese government overcame its concerns about free movement of information and allowed a small academic and scientific network, NetNam, to operate because the government saw the Internet as the "fastest, cheapest way" to improve communications with the rest of the world.[39] The Vietnamese government then apparently had second thoughts about unregulated communications and decided to set up its own system using hardware purchased from a U.S. telecommunications company, Sprint. The new system, which is likely to displace NetNam, will have a greater capacity, but Nghiem Xuan Tinh, deputy director of Vietnam Data Communications Company, itself a subsidiary of Vietnam Post and Telecommunication, has stated that the government hopes that it will be controlled more tightly than "for technical and security reasons [and] from the cultural aspect."[40] The government intends to keep out foreign pornography and other harmful information sent by "foreign organizations."[41] Indeed, anti-communist emigrés based in California have already tried to overwhelm the Vietnamese Prime Minister's e-mail inbox.[42] A government spokesman admitted, however, that the government was uncertain as to how it would achieve its goals, but he promised that the government intended to "think about it."[43]

In Singapore, the government has promised penalties for anyone caught transmitting pornographic or seditious matter.[44] It has also ensured that its point of view will be represented in a Usenet discussion group, soc.culture.singapore, frequented by its critics. Government spokespersons routinely post messages giving the official view of issues.[45] Overall, however, the government has chosen to control Internet access since, despite its best efforts, it cannot figure out how to control content:

> The Singapore government knows that it cannot do much to censor the Internet. But it refuses to give up without a fight.

> The main control is to limit access—the rationale being that only the determined would get at the materials and not the casual users. ...
>
> Singapore's case is instructive in that it is trying to both control information and yet benefit from the Information Age. Current thinking suggests that it is difficult, if not impossible, to achieve both aims. Nevertheless, Singapore is trying.[46]

As part of its campaign against Internet pornography, the Singaporean government searched the files of users of Technet, one of Singapore's major Internet providers. A scan of 80,000 graphics files identified by the extension ".gif" in the file name found five pornographic files, resulting in warnings to their owners.[47] Foreign companies with offices in Singapore became concerned that the Singaporean government would feel free to search their data in the hopes of finding confidential corporate e-mails, and the government had to promise them that it would not conduct such a wide-ranging search again.[48] Meanwhile, one Internet provider in Singapore has promised to block access to "illegal" Web sites.[49]

Other Asian nations have expressed similar concerns about the Internet. The Malaysian government, for example, is studying regulations to penalize those making disparaging remarks about the country on Web pages or in USENET discussion groups.[50]

The People's Republic of China is a special case because although it is industrializing rapidly and its government appears to be committed to increasing Internet access, the government also appears to be intent on retaining the highest possible degree of state control.[51] Although Internet usage is growing quickly on both campus and commercial servers, albeit from a low base, the Chinese government is seeking to limit Internet access by keeping the costs of local service artificially high while it formulates a long-term policy.[52] China's post and telecommunications minister, Wu Juchuan, recently announced that "as a sovereign state China will exercise control" over information. "By linking with the internet, we do not mean the absolute freedom of information."[53]

A sufficiently determined totalitarian government might be able to achieve considerable control over its citizens' use of the Internet by some combination of strict access control, a ban on unlicensed cryptography, random monitoring of stored data and communica-

tions, and draconian punishment for sending or receiving unapproved materials. In time, it might also be possible to create tiered access to foreign materials. Behind this hypothetical Great Firewall of China, most users would be allowed to exchange information with foreign sites if they were on the approved list; controls on domestic information exchange might also be possible, although they might be prohibitively expensive unless the default rule were to be no communication at all. Even a firewall aimed only at controlling the content of international communications would require a very significant investment in filtering software and in manpower to keep the approved site list up-to-date, although it might be able to use simple content analysis to filter out some probably troublesome data (e.g., specific banned words or phrases). A content firewall would reduce the economic value of the Internet considerably. Furthermore, since it is impossible to filter only objectionable material, the system will either filter too little or too much. The tighter the filter, the greater the opportunity cost in lost ability to access the rest off the world's data. Nevertheless, a very aggressive firewall combined with the *in terrorem* effects of some well-publicized punishment of violators might at least allow the government to discourage a large fraction of unsanctioned international information exchanges.

In order for such a strategy to have any hope of success, however, the government must be prepared to resist domestic pressure, pressure from abroad, and especially pressure from foreign firms with local offices that, like those established in Singapore, are likely to protest loudly at having their data and communications monitored. The Chinese government's reassertion early in 1996 of the state news agency's monopoly over the transmission into China of all news and business information[54] is only the latest incident suggesting that the Chinese government may be uniquely willing to stand up to such pressure.

A Canadian Example: the Karla Homolka Case

A lurid example of the difficulty of censorship comes from the failure of the Canadian government to control coverage of the criminal trials of Karla Homolka and Paul Bernado. Canadian law

imposes a strict blackout on news coverage of criminal trials so that news coverage will not influence criminal juries, which are not sequestered.[55] On July 5, 1993, a Canadian judge entered an order banning publication of anything relating to the sensational sex-murder trial of Karla Homolka in order to avoid prejudice to the forthcoming trial of her accused former husband and accomplice, Paul Bernado.[56]

Within days, Canadians had formed a Usenet group, alt.fan.karla-homolka, which began to carry foreign press accounts of the trial and the cases. Some Canadian universities sought to comply with the court order by deleting the newsgroup from their servers. This may have protected the universities from charges that they were complicit in evading the ban, but it was a futile gesture from the point of view of blocking access to alt.fan.karla-homolka since Canadians, including those connected to Internet-enabled computers at those same universities, could read the same Usenet group by connecting to foreign computers. The Usenet group was soon supplemented by a mailing list, Teale Tales, that e-mailed the details of the trials to Canadians chafing under a blackout that successfully covered newspapers, broadcast media, and cable television.[57] The list, which apparently was run by one or more Canadians, originally used the pseudonymous remailer at anon.penet.fi; at its peak Teale Tales accounted for 90% of the traffic passing through that remailer.[58] When the volume threatened to overwhelm the Finnish remailer, the list moved to a computer in the United States. Although the Canadian government prosecuted persons who broke the publication ban by photocopying and distributing paper copies of foreign articles and videotapes of U.S. news programs,[59] it does not appear to have prosecuted anyone involved in electronic distribution.

Costs and Limits of Uncontrolled Speech

The inability to enforce a ban on anonymous Internet communication will impose real costs in untraceable libel, hate speech, and (perhaps) theft of intellectual property.[60] Despite these considerable costs, at a global level the net effect of untamable anonymous speech is likely to be positive: as we have seen, anonymous commu-

nication spells the end of restrictive national policies regarding information. Any government that allows its citizens to become a part of the global electronic network will be forced to live with a freedom of speech even greater than that contemplated by the authors of the First Amendment. The Singaporean example suggests that the ability of any but the most authoritarian government to restrict access to the global information network is limited because businesses value unrestricted access. No democracies, and indeed few other nations, are likely to be as determined and technically adept as Singapore.

Even so, governments are not yet powerless. Governments have it within their power to impose some costs, at least in ease of use, on those who wish to communicate anonymously. However, a country that wishes to ban electronic mail to or from foreign anonymous remailers will find violations hard to detect unless it expends great resources on monitoring all national traffic. Even if monitoring is tried, the monitors will find it difficult to distinguish between ordinary mail and mail to anonymous remailers unless the government either bans encryption or maintains a very up-to-date list of foreign remailers. Indeed, many nations are trying to control the use of cryptography. Such efforts, if successful, make it much more difficult for citizens to communicate anonymously. For example, both France[61] and Russia[62] have relatively comprehensive controls on the use of cryptography—at least on paper. There is as yet little evidence that these laws have had much impact on behavior. A ban on cryptography can in any event be circumvented—at some cost to ease of use—by employing steganography, which is "the art and science of communicating in a way which hides the existence of the communication." Using steganography Alice might hide her messages to Bob inside a an innocuous photograph, encoded in a way that an observer could not even detect that there was a secret message present.[63]

Once a nation's citizenry generates too much traffic to monitor in any systematic way, the prime effect of a single government's attempt to ban anonymous messages will be to make anonymous communication much less easy to use for those concerned about getting caught. Loss of ease of use is a significant factor because the harder a computer technique is to use, the fewer people will use it.

Furthermore, the more difficult a computer technique, the more frequently users will make sloppy mistakes that could lead to their being detected. The leading study of "how cryptographic systems fail in practice" concluded that "many products are so complex and tricky to use that they are rarely used properly. As a result, most security failures are due to implementation and management errors."[64] Criminalization drives use at least partly underground, much like the attempt to control drugs has no doubt reduced but in no way eliminated the use of marijuana and narcotics in the U.S. and other countries.[65] Users of illicit cryptography may be unable to find quality technical support that would help them avoid sloppy mistakes, further increasing the chance of detection.

Despite these real constraints, widespread access to anonymous communication, even if the communication carries some risk, means that citizens armed with computers will be able to criticize their government—and denounce their neighbors—with less fear of retribution than ever before and will have increased access to messages from around the world giving alternative points of view. Meanwhile, at this writing there is little or no risk involved in using a chain of anonymous remailers, and only a little technical skill is required.

As a result, rules seeking to control the export of information such as the International Traffic in Arms Regulations (ITAR) will become ever more difficult to enforce.[66] Again, the Karla Homolka case is instructive. The remailers running the Teale Tales mailing lists were located outside Canada; the case thus demonstrates the difficulty the Internet presents for those charged with keeping information from pouring into a country. But the Homolka saga also demonstrates how hard it is to keep information from escaping across borders: the stories carried on the Teale Tales list and on alt.fan.karla-homolka originated inside Canada. Some were exported by foreign journalists who published in their home newspapers; some were exported directly by Canadians themselves taking advantage of pseudonymous or anonymous remailers.

In the absence of strong international cooperation, the existence of anonymous remailers means that rules seeking to limit the importation of "subversive" or "obscene" speech become impossible to enforce consistently while the recipient country remains

connected to the Internet. Like it or not, we live in an age of completely free speech—of one limited and anonymous type—for everyone with access to a computer connected to the Internet.

Increased Transactional Freedom

A border that is porous to "subversive" speech is also open to transactions in which no physical goods are exchanged. Widespread connection to the Internet is thus likely to increase the citizen's ability to opt out of regulatory regimes in certain limited types of commerce. Already, we see transborder gambling and the sale of digital pornography; in time one can reasonably expect to see some transborder trade in other types of information and value-added information services, such as software, editing, and perhaps even securities and other financial transactions. These transactions may be structured to evade taxes or regulations imposed by the jurisdiction in which the customer resides; without cooperation between the two governments involved, however, there may be relatively little that the government whose rules are being flouted can do about what will, in most cases, be victimless crimes without a complaining witness.

Many states have laws against gambling generally or against private gambling; gambling debts are often not enforceable in court. A number of offshore services now advertise their willingness to take bets via the Internet with payment by credit card or electronic cash.[67] Whether the bettor commits an offense by placing a bet abroad is a question of the law of her home state. As a practical matter, it seems unlikely that the government of the bettor's jurisdiction will be able to learn of the offense without either intercepting the communication, unraveling the payment mechanism, or securing the cooperation of the authorities in the bookie's jurisdiction. If the bookie is established in a jurisdiction where private betting is legal and that jurisdiction requires dual criminality, this cooperation is unlikely to be forthcoming.[68] Indeed, if the bookie fails to pay, the debt is likely to be enforceable in his jurisdiction. Similarly, images deemed obscene in one jurisdiction may be legal elsewhere. Since the information can be encrypted, there is little to prevent international traffic in Internet pornography, which in fact already exists.

Although the traditionally illicit businesses have been the pioneers, it seems likely that in the not too distant future other kinds of transborder information transactions will be conducted electronically. Once an electronic cash infrastructure is in place, there will be few practical obstacles to e-cash being used to trade securities, although consumers might have legitimate fears about their ability to secure redress cost-effectively against a foreign-based broker. Where, however, a jurisdiction has regulations that significantly impede the transactional freedom of its citizens or that impose sufficiently large costs on those transactions as to make offshore brokerages appear worth the added risk, one can expect to see significant regulatory arbitrage between securities markets. Alternately, some customers may choose to trade in jurisdictions that offer them more protection against their brokers than is available at home. Whether this form of regulatory arbitrage will result in a "race to the bottom" toward unregulated markets or a "struggle to the top" to more regulated and perhaps more secure markets is impossible to say;[69] the key points are that there will be greater competition between markets and that this competition will impose constraints on the regulations that governments can introduce without securities trading flowing overseas.

Mobility of Personal Data

The international nature of data flows limits the ability of any single nation to enforce its data protection laws.[70] (Whether data protection laws are effective in providing long-term protection of the privacy of personal information is in any case uncertain.[71]) As a result, the European Commission now allows transborder data flows only if the recipient country offers "an adequate level of data protection."[72] However, even a highly organized international effort to control data flows could be undermined by a *data haven*—the information equivalent to a tax haven—a single nation that offers to warehouse data.

The existence of a data haven would undermine data protection laws in several ways. It could be used to store information about individuals that was illegal to store elsewhere. The owners, or the clients, could engage in massive "data mining" to cross-index that information.[73] It could either market the data to companies unable

to compile the data themselves, or firms located in the data haven could provide services—for example, direct marketing, detailed asset information, or consumer profiles—that companies located elsewhere are forbidden to acquire or provide. The new European directive on transborder data flows recognizes the international nature of the data protection issue,[74] but even Europewide regulation is insufficient. European law forbids the export of personal data to states that do not provide adequate privacy protection. Personal data, however, are notoriously leaky. Furthermore, once information leaks or is quietly sold to a firm located in a data haven, it may be difficult to trace the leak to its source, and it is likely to be impossible to take action against firms located in the haven. Europe, at least, is making an effort to confront the international aspects of the issue; U.S. law remains mired in the single state paradigm.

It is difficult to see, however, how even a multilateral convention would solve the problem of data leakage unless the convention required participants to subject non-complying states—states that would presumably refuse to join the convention—to very strict penalties. Arguably, nothing less than a world willing to impose severe sanctions on nonparticipants, such as cutting off all telecommunications to them, might suffice, and it is difficult to imagine that a strong enough consensus will emerge to impose such sanctions.

No End to Taxes

Although the implications of anonymous transactions for taxes, product liability, and copyright remain to be worked out, it seems likely that the effects of anonymity will be unevenly distributed. Despite dire warnings to the contrary from some tax authorities, I do not believe that the tax system will be deeply affected by anonymous communication or even anonymous electronic cash since most production and even more consumption involves transactions that are easily monitored for tax compliance. Few of the electronic cash systems offered today include sufficient anonymity to allow tax evasion. Current digital cash systems that rely entirely on software are either not anonymous at all or anonymous only for

the payor because the issuing bank always knows the identity of the recipient of the currency. Some electronic cash systems currently being tested use hardware tokens (e.g., smart cards) and are theoretically capable of anonymous peer-to-peer fund transfers. There is, however, no evidence that the owners of these systems intend to enable that capability.[75]

For salaried workers, income tax noncompliance requires payors as well as payees to participate in circumventing reporting requirements. Widespread deduction and reporting of tax at source makes this unlikely. My salary, for example, is paid by an institution that has no incentive to make it easy for me to engage in tax avoidance. True, the prevalence of salaried workers may be lessening; the U.S. economy is said to be shifting toward smaller-sized businesses. But as the numbers of owner-operated businesses and independent contractors increase, the potential for tax fraud grows whether payments are electronic or not. Although some knowledge workers may be able to demand that payment be routed to accounts held at untaxed offshore addresses, thus causing an effect at the margin, I predict such schemes will remain marginal for the foreseeable future.

Furthermore, any transaction that encounters the banking system—for example, short-term deposits—will be easily traceable for tax purposes as long as the bank is located in a jurisdiction that enlists banks as enforcers of its (and perhaps its treaty partners') tax rules. Few nations offer strong banking secrecy today, and the international effort to curb money laundering has reduced their number;[76] some nations that continue to offer strong banking secrecy may lack the political stability necessary to lure risk-averse investors. Conceivably, the tax system might begin to feel the effects if a reputable bank in a country with a stable currency and a trustworthy regulatory system were to offer anonymous electronic cash accounts on terms attractive to ordinary consumers. In that event, other countries would still be able to mitigate the effects by switching to a Value Added Tax (VAT) system since tax cheating under a VAT system would require the participation of more people in the chain of production. Furthermore, the same technology that would enable tax cheating would vastly enhance the capability of tax collectors to amass transactional data about citi-

zens; if the state is willing to collect this data aggressively, tax cheating may actually become more difficult, not more common.[77]

Little Effect on the "Police Power" over Tangible Goods

Finally, it almost goes without saying that most regulation of tangible goods (known in the U.S. as "police power") will remain unaffected by the Internet. Food and drug regulation does not change because research chemists have new ways of communicating. Traffic laws, pension laws, tort law, indeed vast tracts of the legal and social landscape, will no doubt change in the future—but not because of the Internet.

Only if the Internet were to change migration patterns would the Internet significantly alter traditional regulations. Workplace safety rules need not change to lose their effectiveness if the workplace moves. It may be that certain types of knowledge workers based in low-wage areas will be able to increase the market for their services. Mathematicians and programmers have already begun to exploit this opportunity;[78] perhaps editors and artists will be next. As the Internet becomes the leading means to rapidly disseminate scientific, technical, and even social information, people in less developed countries who find themselves isolated in provincial areas or are concerned about keeping abreast of developments in their field may conclude that they no longer have to move to more developed countries and regions to do cutting-edge work or to participate in scholarly exchanges. Consider, for example, the sense of isolation reported by theoretical physicist Abdus Salam upon his return to Pakistan after years in Cambridge and Princeton's Institute for Advanced Studies.[79] An Internet connection does not provide the ambiance of Cambridge or Princeton, but it would lessen the isolation. The increased ability of some persons in traditionally low-wage areas to sell their services on the world market and participate in global dialogues may help stem the so-called "brain drain." Indeed, it may increase the phenomenon of "reverse brain drain" as some expatriates return to their country of origin, perhaps even joined by a new wave of expatriate knowledge workers seeking a lower cost of living.

The Internet as a Promoter of Liberal Democratic Values

For the foreseeable future, the net effect of the continuing internationalization of the Internet will probably be to promote liberal democratic values of openness and freedom and not to detract from modern states' legitimate regulatory powers. Indeed, there is empirical evidence that information interconnectivity is a "powerful predictor of democracy."[80]

The Internet thus continues, even accelerates, a trend that started with CNN. The world's eyes—those of its people as well as its governments—are increasingly acute, omnipresent, and rapidly focused. Globalized communications have already transformed the politics of several countries. For example, electronic mail is credited with contributing to the failure of the 1991 coup attempt in Moscow.[81] Fax communication and the presence of CNN's cameras limited the Chinese government's ability to suppress the Tiananmen Square protests of 1989.[82] The U.S. government's awareness of the presence of TV cameras has greatly shaped the tactics of every foreign military operation since Vietnam.[83]

In the medium term, the existence of anonymous remailers and jurisdictions willing to host them means that communicative anonymity is an inevitable consequence of allowing citizens access to the Internet. The Internet's ability to make everyone with access a secret publisher as well as a secret reader spells the end of censorship for any government that permits widespread access to the Net. As the recent posting of a banned issue of the Zambian *Post* in early 1996 suggests,[84] this phenomenon is already spreading to nations with limited Internet connections. And as the Singaporean example suggests, the costs of denying access will be intolerable to most governments. Access is not costless: regulatory arbitrage will make some regulation, such as the control of digital gambling and pornography, next to impossible and will likely complicate the regulation of information commerce generally. Nevertheless, the state's power to tax and the vast majority of its police power will remain largely unaffected.

Totalitarians will fare worst in this new world, as they will be forced to choose between, on the one hand, limiting access and paying a substantial price in economic growth[85] or, on the other

hand, letting go of their control of information, a traditional tool of social control. Libertarians will not, however, find that their promised land naturally materializes, since the effects of regulatory arbitrage are concentrated and leave most of the traditional regulatory functions of the state untouched. Liberal democrats, however, should be pleased since the increase in international communication will promote the emergence of a global civil society[86] and enhance democratic values of openness and citizen participation while making censorship ever more costly to the national well-being of censors.

Not that all is necessary rosy: to know your neighbors is not necessarily to love them.

Notes

1. Thomas Bullfinch, *Bullfinch's Mythology*, ed. Richard Martin (New York: Harper Collins, 1991), p. 130; Edith Hamilton, *Mythology* (New York: New American Library, 1942), p. 231.

2. Information Sciences Institute, University of Southern California, "Internet Protocol" (Network Working Group, Request for Comments No. 791, September 1981), http://ds.internic.net/rfc/ rfc791.txt; Information Sciences Institute, University of Southern California, "Internet Protocol" (Network Working Group, Request for Comments No. 793, September 1981), http://ds.internic.net /rfc/rfc793.txt; Gary C. Kessler and Steven D. Shepard, A Primer On Internet and TCP/IP Tools (Network Working Group, Request for Comments No. 1739, December 1994), http://ds.internic.net/rfc/rfc1739.txt (describing major TCP/ IP-based applications); Vincent Cerf and R. Kahn, "A Protocol for Packet Network Interconnection," in *IEEE Trans Communications*, vCOM-22n5 (May 1974), p. 637.

3. David H. Crocker, "To Be 'On' the Internet" (Network Working Group, Request for Comments No. 1775, March 1995), http://ds.internic.net/rfc /rfc1775.txt.

4. Bruce Sterling, "Short History of the Internet" (February 1993), gopher: //gopher.isoc.org:70/00/Internet/history/short.history.of.internet.

5. Ibid.

6. IETF Secretariat et al., "The Tao of IETF 3" (Network Working Group, Request for Comments No. 1718, November 1994), http://ds.internic.net/rfc/rfc1718.txt [hereinafter IETF Tao].

7. Paul Mockapetris, POISED '95 BOF gopher://ds.internic.net/00/ietf/95apr /poised95-minutes-95apr.txt.

8. Internet Activities Board & Internet Engineering Steering Group, "Internet Standards Process," Revision 2 at 7 (Network Working Group, Request for Comments No. 1602, March 1994), http://ds.internic.net/rfc/rfc1602.txt [hereinafter RFC 1602].

9. David H. Crocker, "Making Standards the IETF Way," 1 *StandardView* 46, 51 (September 1993), http://info.isoc.org/papers/standards/crocker-on-standards.html.

10. Gary H. Anthes, "Summit Addresses Growth Security Issues for Internet," *Computerworld*, April 24, 1995, p. 67.

11. Bernard Aboba, "How the Internet Came to Be," in *The Online User's Encyclopedia*, gopher://gopher.isoc.org:70/00/internet/history/how.internet.came.to.be.

12. Network Wizards, "Internet Domain Survey," (January 1996), http://www.nw.com/zone/WWW/report.html.

13. Louise Kehoe, "Surge of Business Interest," *The Financial Times*, March 1, 1995, p. XVIII.

14. Donna L. Hoffman, William D. Kalsbeek and Thomas P. Novak, "Internet Use in the United States: 1995 Baseline Estimates and Preliminary Market Segments," http://www2000.ogsm.vanderbilt.edu/baseline/1995.Internet.estimates.html.

15. Nina Burns, "E-mail beyond the LAN," *PC Magazine* April 25, 1995, p. 102.

16. "World-Wide Web," in *The Free On-Line Dictionary of Computing*, http://wombat.doc.ic.ac.uk/?World-Wide + Web.

17. Ibid.

18. Anthony-Michael Rutkowski, Executive Director Internet Society, "Bottom-Up Information Infrastructure and the Internet" (February 27, 1995), http://www.isoc.org/speeches/upitt-foundersday.html.

19. "World-Wide Web," in *The Free On-Line Dictionary of Computing.*

20. I draw out the distinctions between these four types in my "Information Ocean" article. A. Michael Froomkin, "Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases," *University of Pittsburgh Journal of Law and Commerce* 15, (forthcoming 1996).

21. This risk is reduced by the provision of a "remailer pinging service" that regularly checks to see if remailers are forwarding their mail. A list of remailers and their features as well as current information about their recent performance statistics is maintained by a volunteer and published at http://www.cs.berkeley.edu/~raph/remailer-list.html.

22. Anon.penet.fi, probably the best-known "anonymous" remailer, is not in fact an anonymous remailer. It is merely a very user-friendly traceable *pseudonymous* remailer because the anon.penet.fi system keeps a record of each user's e-mail address. The security of the approximately 8,000 messages that pass through

anon.penet.fi daily (see Douglas Lavin, "Finnish Internet Fan Runs Service Allowing Anonymous Transmissions," *Wall Street Journal*, July 17, 1995, p. A7) thus depends critically on the willingness of the operator, Johan Helsingius, a Finnish computer scientist, to refuse to disclose the contents of his index, which maps each anonymous ID to an e-mail address.

In February 1995, the Church of Scientology successfully enlisted the aid of the Finnish police, via Interpol, to demand the identity of a person who, the Church of Scientology claimed, had used anon.penet.fi to post the contents of a file allegedly stolen from a Scientology computer to a USENET group called alt.religion.scientology. Unprepared for the request, Helsingius surrendered the information, believing that the only alternative would have been to have the entire database seized by the police. See http://www.cybercom.net/~rnewman/scientology/home.html#PENET. Differing descriptions of the Scientologists' legal efforts can be found at The Church of Scientology vs. the Net, http://www.cybercom.net/~rnewman/scientology/home.html (critical view); UK Scientology Critics, http://mail.bris.ac.uk/~plmlp/scum.html (even more hostile); Church of Scientology International, http://www.theta.com/goodman/csi.htm (Scientologists' view).

23. Anonymizer FAQ, http://anonymizer.cs.cmu.edu:8080/faq.html.

24. Community Connextion, http://www.c2.org.

25. In a public-key system, each user creates a public key, which is published, and a private key, which is secret. Messages encrypted with one key can be decrypted only with the other key, and vice versa. Whitfield Diffie and Martin E. Hellman, "New Directions in Cryptography," IT-22 *IEEE Transactions Information Theory* (1976), p. 644, and Ralph C. Merkle, "Secure Communication over Insecure Channels," *Communications of the ACM*, April 1978, p. 294; Bruce Schneider, *Applied Cryptography* (New York: John Wiley & Sons, 1994), p. 29; Whitfield Diffie, "The First Ten Years of Public-Key Cryptography," Proceedings of the IEEE 76 (1988), p. 560.

A strong public-key system is one in which possession of both the algorithm and one key gives no useful information about the other key. Anyone in the world can use the public key to send messages that only the private key owner can read; the private key can be used to send messages that could only have been sent by the key owner.

Thus, if Alice wants to send a secure e-mail message to Bob and they both use compatible public-key cryptographic software, Alice and Bob can exchange public keys on an insecure line. If Alice has Bob's public key and *knows that it is really Bob's* then Alice can use it to ensure that only Bob, and no one pretending to be Bob, can decode the message. A strong public-key system makes it possible to establish a secure line of communication with anyone who is capable of implementing the algorithm. (In practice, this is anyone with a compatible decryption program or other device.) Sender and receiver no longer need a secure way to agree on a shared key. If Alice wishes to communicate with Bob, a stranger with whom she has never communicated before, Alice and Bob can

exchange the plaintext of their public keys. Then Alice and Bob can each encrypt their outgoing messages with the other's public key and decrypt their received messages with their own secret, private key. The security of the system evaporates if either party's private key is compromised, that is, transmitted to anyone else.

PGP stands for "pretty good privacy," a type of robust encryption, which when used with a long key is unbreakable in any reasonable period of time by currently known techniques. PGP is available online by FTP from many sites, including ftp://net-dist.mit.edu/pub/, ftp://ftp.ox.ac.uk/pub/crypto/pgp, or a German server: ftp://ftp.informatik.uni-hamburg.de:/pub/virus/crypt/pgp. For a good description of the technical and political workings of PGP, see Simson Garfinkel, *PGP: Pretty Good Privacy* (Sebastopol, CA: O'Reilly & Associates, 1995).

26. A. Michael Froomkin, "The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution," 143 *University of Pennsylvania Law Review* (1995), pp. 709, 747, http://www-swiss.ai.mit.edu/6095/articles/froomkin-metaphor/text.html.

27. Lance Cottrell's home page on Mixmaster: http://obscura.com/~loki/; Remailer-Essay, http://nately.ucsd.edu/~loki/remailer/remailer-essay.html.

28. Spam FAQ, or "Figuring out Fake E-Mail and Posts," http://digital.net/~gandalf/spamfaq.html.

29. Contrary to what some believe, ordinarily there is very little that an e-mail message can do to harm the recipient other than communicate information that the recipient might not desire to know. In any reasonably well-designed software, users do not become susceptible to computer viruses or "trojan horses" merely by reading an e-mail message. Some further action on the recipient's part is required, e.g., attempting to run a program that may have been attached to the e-mail message.

30. Paul A. Strassman and William Marlow, "Risk-Free Access into the Global Information Infrastructure via Anonymous Re-Mailers," http://www.strassman.com/pub/anon-remail.html.

31. Penthouse Magazine, "Not Available in These Countries," http://www.penthousemag.com/resource/nothere.html.

32. Thus Eugene Volokh's radical predictions about the demise of private speech regulation in the United States actually may be too timid because they do not take account of the international nature of the Internet. Eugene Volokh, "Cheap Speech and What It Will Do," *Yale Law Journal* (1995), pp. 1805, 1836.

33. "Redefining Community," *Information Week*, November 29, 1993, p. 28 (quoting Gilmore).

34. Ethan Katsh, "Rights, Camera, Action: Cyberspatial Settings and the First Amendment," *Yale Law Journal* 104 (1995), pp. 1681, 1695 n. 43; George P. Long, III, Comment, "Who Are You?: Identity and Anonymity in Cyberspace," *University of Pittsburgh Law Review* 55 (1994), pp. 1117, 1186–1187 (describing operation of "Automatic Retroactive Minimal Moderation").

35. A. Michael Froomkin, "The Importance of Trusted Third Parties in Electronic Commerce," 75 *Oregon Law Journal* 75 (forthcoming, 1996).

36. Katsch, "Rights, Camera, Action," p. 1695, n. 43.

37. Canadian Copyright Act §14.1.

38. Philip Shenon, "2-Edged Sword: Asian Regimes on the Internet," *New York Times*, May 29, 1995.

39. Ibid.

40. Jeremy Grant, "Vietnamese Move to Bring the Internet Under Control May Backfire," *Financial Times*, September 19, 1995.

41. Ibid.

42. Shenon, "2-Edged Sword."

43. Grant, "Vietnames Move to Bring the Internet Under Control May Backfire."

44. Shenon, "2-Edged Sword."

45. Philip Taubman, "Cyberspace in Singapore," *New York Times*, November 8, 1995.

46. Peng Hwa Ang and Berlinda Nadarajan, "Censorship and the Internet: A Singapore Perspective," http://info.isoc.org/HMP/PAPER/132/txt/paper.txt (the lead author is a professor at the School of Communication Studies, Nanyang Technological University) [hereinafter "Singapore Perspective"].

47. Ibid.

48. Shenon, "2-Edged Sword."

49. "Asianisation of the Internet Predicted," http://www.jaring.my/star/friday/22nett.html (article from Malaysia Star Online).

50. Posting from Dave Farber to "interesting-people mailing list" March 12, 1996.

51. Joseph Kahn et al., "Beijing Seeks to Build Version of the Internet that Can Be Censored," *Wall Street Journal*, January 31, 1996; Tony Walker, "Beijing Tightens Rules on Access to Internet," *Financial Times*, February 5, 1996.

52. Shenon, "2-Edged Sword."

53. Tony Walker and Shi Junbao, "China's Wave of Internet Surfers Sets Censors a Poser," *Financial Times*, June 24, 1995.

54. Tony Walker, "China Threatens Flow of Business Information," *Financial Times*, January 18, 1996.

55. Criminal Code of Canada §486(1)

56. [1993] O.J. NO. 2047, Action No. 125/93, [R. v. Bernardo].

57. Paul Bernardo Teale/Karla Homolka Frequently Asked Questions List (FAQ) Version 4.0, January 12, 1995, Part One, http://www2.magmacom.com/~djakob/censor/karlafaq.txt.

58. Ibid., p. 5.

59. Ibid., §2b.

60. Technical countermeasures, akin to salting each copy of the telephone book with unique false entries to pinpoint the source of any copies, may reduce attractiveness of unsanctioned copying of digitized information. In addition, customers may prefer to buy products from vendors they know and trust. For example, someone posted code on the Internet that produces output identical to RC4, a propriety encryption algorithm of RSA Data Security, Inc. A spokesman for the company stated that sales of RSA licensed products were not affected by this apparent leakage of intellectual property because customers wanted the confidence of dealing with a reputable supplier. Telephone interview with Kurt Stammberger, Director of Technologies Marketing, RSA Data Security, Inc., November 22, 1995.

61. The French rules derive from Law No. 90-1170 (*Journal Officiel*, December 20, 1990). "Crypto Law Survey," http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm#fr; Ross Anderson, "Crypto Policy by Country," Appendix to *Crypto in Europe—Markets, Law and Policy*, ftp://ftp.cl.cam.ac.uk/users/ria14/queensland.ps.Z.

62. Stepoe and Hohnson, "Edict" (unofficial translation), http://www.us.net/~steptoe/edict.htm; Steptoe and Johnson, "Russian Statutes Restricting Use of Encryption Technologies," http://www.us.net/~steptoe/cyber.htm.

63. Markus Kuhn, "Steganography Mailing List," http://www.thur.de/ulf/stegano/announce.html.

64. Ross Anderson, "Why Cryptosystems Fail," *Communications of the ACM* 37 November 11, 1994, pp. 32–41, ftp://ftp.cl.cam.ac.uk:/users/ria14/wcf.ps.Z.

65. Steven B. Duke and Albert C. Gross, *America's Longest War: Rethinking Our Tragic Crusade Against Drugs* (New York: Putnam, 1993).

66. The true purpose of the ITAR as applied to cryptographic devices and algorithms may be to restrict the emergence of a standard mass-market encryption product. In that case, anonymous communication will not greatly reduce the ITAR's effectiveness. Until anonymous digital cash is widespread, no commercial software publisher in the United States will risk violating the ITAR since there is no effective means for them to charge for their products and yet maintain the anonymity they would require to avoid any risk of prosecution. ITAR page, ftp://ftp.cygnus.com/pub/export/export.html.

67. http://www.box.eu.org/~dl/inc/play.shtml. A list of Internet-based gambling operations appears at http://businesstech.com/guest/howertable.html.

68. For a survey of judicial assistance treaties that waive the dual criminality requirement see James I. K. Knapp, "Mutual Legal Assistance Treaties as a Way to Pierce Bank Secrecy," *Case Western Reserve Journal of International Law* 20 (1988), p. 405.

69. Caroline Bradley, "The Market for Markets: Competition between Investment Exchanges," in John Fingleton ed. (assisted by Dirk Schoenmaker), *The Internationalisation of Capital Markets and the Regulatory Response* (London: Graham & Trotman, 1992), pp. 183–196.

70. Paul M. Schwartz, "European Data Protection Law and the Restrictions on International Data Flows," *Iowa Law Review* 80 (1995), pp. 471, 472 [hereinafter "European Data Protection Law"]; Paul M. Schwartz, "Privacy and Participation: Personal Information and Public Sector Regulation in the United States," *Iowa Law Review* 80 (1995), pp. 553, 612.

71. David H. Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (Chapel Hill: University of North Carolina Press, 1989), pp. 406–407.

72. Common Position (EC) No/95 With a View to Adopting Directive 94/ /EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, 1994, O.J. (C 93, April 13 1995), reprinted in Appendix, *Iowa Law Review* (1995), p. 697; "European Data Protection Law," pp. 480–488.

73. Froomkin, "Flood Control on the Information Ocean."

74. Directive 95/46/EC of the European Parlilament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L281, November 23, 1995).

75. Froomkin, "Flood Control on the Information Ocean," p. 86.

76. Caroline A.A. Greene, Note, "International Securities Law Enforcement: Recent Advances in Assistance and Cooperation," *Vanderbilt Journal of Transnational Law* 27 (1994), p. 635; Dennis Campbell, *International Bank Secrecy* (London: Sweet & Maxwell, 1992).

77. Froomkin, "Flood Control on the Information Ocean," p. 86.

78. See, e.g., Don Clark, "China Challenges U.S. Export Law With Alliance in Code Technology," Wall Street Journal, February 8, 1996 (describing sale of programming and cryptological services by China).

79. Abdus Salam, "Cooperation for Development," in *UNESCO World Science Report* (1993), p. 167, quoted in Markus Schlegel, "Brain Drain With Regard to Africa," http://www.sas.upenn.edu/African_Studies/Articles_Gen/Brain_Drain.html.

80. Christopher Kedzie, "International Implications for Global Democratization," in Robert H. Anderson et al., *Universal Access to E-Mail: Feasibility and Societal Implications* (Santa Monica, CA: The RAND Corporation, 1995), http://www.rand.org/publications/MR/MR650/mr650.ch6/ch6.html.

81. David Lyon, *The Electronic Eye: The Rise of Surveillance Society* (Minneapolis: University of Minnesota Press, 1994), p. 87.

82. See Steven V. Roberts et al., "New Diplomacy by Fax Americana," *U.S. News & World Reports*, June 19, 1989, p. 32.

83. See, e.g., Matthew J. Jacobs, "Assessing the Constitutionality of Press Restrictions in the Persian Gulf War," *Stanford Law Review* 44 (1992), p. 675.

84. See "Zambia's Newspaper Censorship," http://www.cs.cmu.edu/~declan/zambia/news.html.

85. Kedzie, "International Implications for Global Democratization."

86. For some suggestions about this phenomenon see World Alliance for Citizen Participation, *Citizens: Strengthening Global Civil Society* (Washington, DC: CIVICUS, 1994).

 Portions of this paper are revised versions of A. Michael Froomkin, "Anonymity and Its Enmities," 1 *J. Online L.*, Article 4 (1995), http://www.law.cornell.edu/jol/froomkin.html, and of A. Michael Froomkin, "Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases," 15 *University of Pittsburgh Journal of Law and Commerce* (forthcoming 1996). I am grateful to Caroline Bradley and Bernard Oxman for helpful comments.