The Privacy Debate: To What Extent Should Traditionally “Private” Communications Remain Private on the Internet?

Joel Reidenberg
*Fordham University School of Law, jreidenberg@law.fordham.edu*

Norman I. Silber
*Hofstra University School of Law*

Peter D. Kennedy
*George, Donaldson & Ford*

Ronald Abramson
*Hughes, Hubbard & Reed*

Follow this and additional works at: [https://ir.lawnet.fordham.edu/iplj](https://ir.lawnet.fordham.edu/iplj)

Part of the [Entertainment, Arts, and Sports Law Commons](https://ir.lawnet.fordham.edu/iplj), and the [Intellectual Property Law Commons](https://ir.lawnet.fordham.edu/iplj)

Recommended Citation
Available at: [https://ir.lawnet.fordham.edu/iplj/vol5/iss2/3](https://ir.lawnet.fordham.edu/iplj/vol5/iss2/3)
PROF. REIDENBERG: Our topic this afternoon is whether traditionally private communications should remain private when they are on the Internet. This topic raises a variety of themes and we will try to touch on many of them.

Part of our inquiry will examine what the technology is doing and will explore the challenges that the technology poses to us for private communications.

When we look at the technology and the Internet in particular, we see new problems and new issues being raised. How do we use it? If I post a message to something called a Usenet Group or if I simply send a "point to point" e-mail message, it may have radically different consequences for both who can access it, and what else can happen to that message.

The act of sending a message now generates information, gen-
erates details about what I do. If we engage in interactive communications and use multimedia activities, like watching a movie in the privacy of the home, these activities may no longer be private. Now it is possible for others to know what I am watching, or whether I am paying attention to the commercials. Marketers want to know, for instance, if I zap the commercials. Do I prefer beer commercials or do I like the cereal commercials? All of this information has now become accessible through various technological means.

The kinds of issues that we are going to discuss this afternoon can be cast in four different dimensions. The first one, which Professor Silber will lead, is the consumer view. As consumers in society, how does the technology and the marketplace of the technology affect us and how does it affect what we perceive as private?

We will then think about the content of communications. Who has access to what I say or how I say it? Peter Drew Kennedy will discuss this topic, and I will introduce it in more detail when it comes up, but the general issue is how people are protected when they are engaged in communications by means of information technologies.

This also raises issues of cryptography—whether there are self-help mechanisms in addition to legal ones—which Ron Abramson will address. We will also be confronting other related questions, such as whether transaction information is private, and if it is, who owns it. Still other questions are raised through the merger between ownership issues and privacy issues—if I gather the information, can I use it any way I want? We think of these rights as property. Yet, how I use the information may implicate rights that concern individuals.

Finally, I hope that we will touch on questions of the roles of the state and the private sector. How do we set up a regulatory framework? What is the proper role of the state? Should self-regulation prevail? Do we focus on letting the network figure it out for itself? Or should the state be stepping in?

With that I would like to introduce Professor Silber. He is a
professor at Hofstra Law School. He holds his law degree from Columbia University, his Ph.D in history from Yale, and is a graduate of the Washington University in St. Louis. Norm, I think, also holds the distinction of being one of the most thoughtful and nicest members of my law school class. So, with that, I will introduce Professor Silber.

PROF. SILBER: Thank you very much. I must preface my talk by saying that when it comes to the world of the Internet, I am an amateur explorer. I don’t want to hold myself out in as an expert. I do claim some experience, however, in the area of consumer regulation and consumer reform.

When I was asked to appear on this panel, the invitation provided me with the opportunity to address some of the problems that consumers are encountering and are likely to encounter in the future as a result of the transformation in the way in which business is being done. And increasingly, as I will indicate, business is being done on the Internet. I am grateful to the editors of this Journal for the opportunity to present my views.

The conventional ways of consuming—going to the store or shopping by catalogue—are being supplemented with newer ones. These involve buying over the telephone, through the television, and now buying over the Internet. There is a new marketplace, cyberspace, and a new way of merchandising—telemarketing. Predictions have been made that by 1998 there will be a community of fifty million commercial users communicating with one another, and fifty million electronic clients and customers on the streets of the Internet, if by that time the “information highway” is still the appropriate metaphor to use.¹

There are many important effects of this change on consumers. I want to focus on two that I feel are among the most important. I will refer to these as the “New Media” effect and the “New Marketing” effect. Then I will consider several possible legal responses to these effects. I am going to argue that the traditional con-

sumer law enforcement paradigms for confronting ordinary consumer problems hold the most promise for improving conditions for consumer users on the electronic superhighway. And along the way I am going to challenge the view that we can expect much from the privacy paradigm, which I gather has really been an underlying premise of this Symposium.

The first effect, the New Media Effect, has occurred virtually every time consumers have confronted an old selling scheme through a new medium. This effect is especially pronounced when, as in these circumstances, new selling techniques are associated with a whole new kinds of technology.

This happened, for example, during medieval fairs when consumers had trouble figuring out the quality of the cloth that they were buying because it was wrapped up in bolts. It happened during the French Revolution when consumers had to take their chances on bottled wine. It happened again in the 19th Century when brand-name advertising came into being.2

In his oral history of the great depression, *Hard Times*, Studs Terkel has revealed how valuable radio advertising space became after radios became commonplace during the 1920s and '30s.3 Consumers were accustomed to advertisements in newspapers and to pitches from sales people, but they had never before heard radio appeals. It took time for consumers to adjust to the particular problems of exaggerated claims and misrepresentations. Historically, every time a new medium for selling arises, consumers have trouble measuring the truthfulness of sellers who use the new medium.

There is money to be made exploiting those who are slow to catch on, and the law also plays catch-up with respect to outlawing inappropriate conduct and enforcing rules that have been made. To persist with my example, the Federal Trade Commission didn't try to prosecute fraudulent radio ads until after World War II.4

---

4. *Id. See also* Eric Freedman, *The Inside-Out Approach to First Amendment Juris-
Today, by all accounts, consumer fraud on the Internet is rampant. Most of it consists of the classical, tried and true, scam varieties. Some of it is novel. Many of the victims are well educated and intelligent people, bright enough and prosperous enough to buy and to operate personal computers. Others are poor, young and uneducated.

Consider briefly four types of fraud that have regularly surfaced on "the Net":

1. **Ponzi Schemes.** Within the last several months, New Jersey regulators stopped an electronic mail chain letter in which prospects were encouraged to send one dollar each to the top five names on the list and they were supposed to place their name at the bottom and sit back and wait for sixty thousand dollars to roll in. That is a classic variation of an old pyramid selling scheme that goes all the way back to the 1920s and '30s.

2. **Stock manipulation.** The instantaneous communication offered by computers has made some scams, such as stock manipulation, far easier to pull off than ever before. Securities regulators in several states have been trying to halt Internet scams, varying from those which get consumers to commit money to phony money management companies, to those involving the hyping of worthless penny stocks. It is very common now, and very easy. You can simply encourage people to buy these penny stocks and then sell the stock that you had bought earlier at a very high price.

Estimated losses are one million dollars an hour nationwide. Unfortunately, at present, a major target for this scam is generally the elderly.

7. *Id.*
8. Lynn Simross, *The Goods*, L.A. TIMES, Aug. 12, 1994, at E3. A regular "boiler room" scam operation can make one hundred and fifty calls on a good day, whereas computer bulletin boards can contact thousands of people a day. *Id.*
3. Phony merchandise and property scams. "It's scam de jour," one law enforcement officer has stated. "Whether it's someone who poses as a celebrity or who deliberately spreads false rumors, fraud is rampant in cyberspace."

Commercial services like America OnLine, CompuServe, Delphi and the Well have released a host of novices on to the electronic bulletin boards and into the electronic realm. One reporter has stated that, "[f]or this new wave of curious explorers, technology has become an authority figure that isn't questioned . . . . You're looking at a computer screen and you forget that you're actually dealing with other people, not some omnipotent being."

Millions of dollars have been lost by Internet newcomers to experts in fraud who purport to sell everything from time-shares to cubic zirconium. The targets of this fraud, for the most part, are people who are new to the medium, and there is the problem of fraud against vulnerable groups, particularly the elderly, but I suspect children as well.

4. Impersonations. Another common scam is impersonations. Thousands of e-mail messages are intentionally being misattributed. Here is a story from the Los Angeles Times:

"You pop on to your America Online account, check your e-[m]ail and find a note from Keanu." The message details how he loves motorcycles, misses River Phoenix and enjoys playing bass in a band called Dogstar. You pull up Keanu's on-line biography—something every AOL member fills out when signing up with the service—and the name listed is KReeves. Even the birthday shown—Sept. 2, 1964—matches the actor's. So, it's got to be legitimate, right? Wrong. On line you can be anyone, with any age and background, and some enjoy fooling others by posing as celebrities. On America Online, three subscribers are posing as U2 singer Bono and four as Keanu Reeves.

11. Id.
12. Simross, supra note 8, at E3.
Times sent e-mail notes to the four Reeves wanna-bees, asking “Are you the Keanu Reeves star of the film ‘Speed’”? Three responded with a yes. One using the handle “Keanu” wrote back that he “picked up lotsa chicks this way.” The real Reeves has never gone on line. In a statement, the actor said he is “appalled” and will “explore any and all legal action” to halt this misrepresentation.

You could argue that this kind of behavior is defamation, and that the other swindles that I have talked about are other varieties of commercial fraud. But how do victims find the parties who are doing the defrauding?

Although these techniques are for the most part time-honored fraudulent schemes, the standard investigative approaches are proving to be ineffective, and the currently necessary evidentiary proofs are hard to come by. For the most part, a person sending information on the Internet can determine what the receiver, or anyone who intercepts the message, will see as the “from” address. This includes not giving any return address at all.

Shouldn’t the Internet service providers bear responsibility for permitting these frauds to operate freely? Why aren’t membership applications being verified and accurate addresses aggressively insisted upon? Shouldn’t those who facilitate the sending of false and misleading messages, especially commercial ones over the network, be punished?

America Online places the responsibility for misrepresentation squarely with its subscribers. “They agree not to submit or display

---


14. See e.g., Michael P. Dierks, Computer Network Abuse, in Symposium: Electronic Communications and Legal Change, 6 HARV. J. L. & TECH. 307, 315 (1993). Dierks describes an example of one person, Kevin Mitnick, who circumvented computer security, causing $4 million in damage to the Massachusetts-based Digital Equipment Corporation through his Los Angeles-based computer. He devised a method of escaping telephone tracing through the use of the call-forwarding service of the telephone company and was able to evade law enforcement officials by re-routing traces on his telephone to any other number of his choosing. Id. at 315-16.

15. John Markoff, Cyberburglars are Using New Methods, HOUS. CHRON., Jan. 23, 1995 (Business), at 5.
any inaccurate information,” a spokesperson stated.16 “If a falsehood is brought to our attention, then we’ll try to deal with it. But we’ve got more than a million subscribers now. It’s impossible for us to track every user. It’s up to people on the service to police themselves.”17

Is this the right outcome? Shouldn’t we shift the loss allocation rules a bit to encourage more attention to these problems by the service providers?

The second major effect of cyberspace on consumers that I want to talk about has resulted not directly from the new salesmanship on computer, but instead it has resulted indirectly, from the use that sellers and marketers in and out of cyberspace can make by sifting through communications and transactions that take place on the Internet.

The sophistication of the marketing has increased to the point at which successful salesmanship and consumption engineering depends on building models of consumer behavior. These models, in turn, depend on capturing information about consumers that is as accurate and as detailed as possible.

The author of the book Doing Business on the Internet states that by following the discussions that occur in user groups it is possible to reveal quickly which groups are a good match for a particular company.18 Another commentator notes that, “even without posting a message, companies will learn a lot about the norms and culture of the network by monitoring a number of groups.”19

There are two ways that the Internet facilitates the capture of marketing information. First, there is the use of the Internet to get into computer databases in order to obtain information. The types of information that can be acquired through an Internet computer connection from databases and lists over ordinary phone lines are

17. Id. (quoting America Online spokeswoman Pam McGraw).
quite astonishing. Most of the information gathered by the private sector remains unregulated, and most efforts to regulate it that exist are voluntary.

Ironically, if you want to avoid inadvertently revealing facts about yourself, it appears that what you have to do is to falsify your name to a service provider, thereby giving a false name and address to marketers.

It should be kept in mind that the Internet is only part of what is becoming a national information infrastructure which will be a web of databases and computer networks. Screening data, sorting it and combining it into lists for solicitations is greatly facilitated by the infrastructure. As we speak, people are sitting at their PCs and Macs and doing aggregation of data and amalgamation of data and acquiring a lot of information.

Jeffrey Rothfelder, an author and reporter for Business Week, managed to get such information as Dan Rather’s credit card data and his home loan mortgage information, and Dan Quayle’s private address and his clothing habits. One wonders what for, but that is another question.

In most cases the information that is obtained is used to identify potential customers who fit a prescribed marketing profile. Marketers are always looking for new card members, buyers for catalogues, and members for their organizations. But so far there

20. John Markoff, A Most Wanted Cyberthief is Caught in His Own Web, N.Y. TIMES, Feb. 16, 1995, at A1. Individual “hackers,” furthermore, have the capability to capture and store information that formerly was exercised only by large institutions. Id.. The databases are everywhere, guarded with widely varying degrees of effectiveness. Id.


22. Judith Waldrop, The Business of Privacy, AM. DEMOGRAPHICS, Oct. 1994, at 46. Also known in the direct mail industry as “merge and purge,” these aggregation methods encompass techniques where information gatherers combine lists and sort them based on assumptions made, such as a person’s wealth, a zip code, or personal lifestyle indicators. Id.

23. JEFFREY ROTHFELDER, PRIVACY FOR SALE 17-18 (1992). In most cases, however, the information that is obtained is used to identify potential customers who fit a prescribed marketing profile. It helps to direct catalogs and products to the people who want them. So far, there aren’t any rules attached to individuals. Id. at 17.
aren't any rules attached to rummaging around.

The second way that cyberspace is affecting consumer marketing is the use by the Internet service providers of their privileged places, alongside the information highway, to collect data themselves. Capturing information on the Internet allows sellers to focus their activities on those that will be most profitable for them and to reject transactions with consumers who might lose them money or cause them trouble.

The services require consumers to execute blanket releases which permit the trading and collection of data to go on as a matter of routine. Let me quote from a standard form contract that subscribers to the Internet service Delphi are asked to sign:

Unless you instruct us otherwise for any reason, on occasion we may arrange with third parties to provide you with information and materials we believe you would enjoy receiving based on your demonstrated interests. Use of the information you provide Delphi Internet may be used for internal, external or commercial purposes, and may involve disclosure of the information to commercial and/or governmental entities.

24. Not only service providers but software manufacturers can collect data. For example, Microsoft Corporation's "Windows 95" software will contain a "registration wizard" feature that would allow the corporation to inventory hardware components and software programs already installed in the user's computer. See, Technology: On Line, N.Y. TIMES, June 19, 1995, at D3.

25. Membership Agreement, Delphi Internet Services Corporation, received Feb. 9, 1995. The agreement also provides that:

- You authorize Delphi Internet to apply all incurred fees to your credit card.
- You agree to be fully responsible for such charges. A credit limit, established by Delphi Internet and by the issuer of your credit card may be applied to your account. Delphi Internet reserves the right to suspend your access to the service if you exceed your credit limit, or upon an indication of credit problems including delinquent payments or rejection of any credit card charges.

*Id.* In addition, the Agreement outlines numerous other rules and limitations. The section on "Rules of Online Behavior" prohibits members from posting any "unlawful, libelous, threatening, abusive, disruptive, or obscene material or message that would violate the rights of any person or constitute a criminal offense, or otherwise violate any local, state, national, or international law." *Id.* Use of distribution lists in electronic mailings is "subject to the approval of Delphi Internet," and members are "prohibited from uploading or reproducing any information protected by copyright without obtaining permission of the
If I were teaching my course in consumer law I would ask, isn’t that a classic example of great psychological framing? Haven’t we framed the question in a way that makes it very unlikely for a consumer to object to having his information used in that way? In other words, the response to this contract language might be very different if it stated something like, “Delphi can do what it wants with whatever you send over the Internet, and can trade your name with third parties unless you negotiate different terms.”

It is also true where the “learning curve” associated with adjusting to a new service provider is steep. Consider the case of an insurance company that uses your health bills and your insurance claim forms to screen offers for further insurance. If people think that their relationship is with their HMO, they have no expectation that their information is going to be distributed to others, and the waiver allowing their information to be distributed is not often framed in a way which could alert them to such a potential use. Technically, I think that most consumers don’t know that offensive use is part of the bargain, and if they did know, they would change that term.

The potential injury to consumers from the conveyance of rights to this information to others can be, and frequently is, severe.

Let me mention a few different categories of injury with which many of you may be familiar. The first is impermissible discrimination. Of great concern is the possibility that this technology can be used illegally or covertly to screen people for jobs, mortgages, insurance or other opportunities. Do you want to know how often somebody has been to the doctor? Do you want to know how often they have been to a motel room? Do you want to know if a caller who wants to rent from you lives in an affluent community or in low income housing?

Some discrimination is lawful but none the less questionable as a matter of social policy. To improve its own risk, Metropolitan Life Insurance Company is now screening individuals at risk for heart disease by scanning HMO claims for diagnosis codes that
identify people who have hypertension or high levels of cholesterol.\textsuperscript{26} They send them a letter and a booklet advising them of the importance of managing their disease.\textsuperscript{27} An employer might similarly try to avoid hiring heart-attack-prone employees. Perhaps an insurer can “cherry pick” by learning who buys steaks at the supermarket, or AIDS medications at a drug store.

The second area of potential injury is where the conveyance of information results in factual mistakes about the consumer. The possibility is always present that incorrect or “misaligned” consumer information is going to be used against the consumer. A market information provider may combine information incorrectly, or in some cases, the combination may produce results that are not consistent. It may be that the information is sufficiently accurate for the marketer to want them, but insufficiently accurate for a consumer to be satisfied with the conclusions that are drawn.

A third area of potential harm is offensive communications: neo-Nazi groups spreading literature to Holocaust victims, anti-abortionists getting hold of Planned Parenthood lists, etc. Oral Roberts acquired a list of deadbeats from an agency and he sent them each a letter, asking them to turn around their lives by sending him a gift of one hundred dollars. He then promised to intercede with God on their behalf and begin what he said was the “war on [your] debt.”\textsuperscript{28}

\begin{itemize}
\item \textsuperscript{26} See Waldrop, \textit{supra} note 22, at 46.
\item \textsuperscript{27} \textit{Id.}
\item \textsuperscript{28} \textit{Id.} As Waldrop points out, however, the mail marketers themselves realize that there is a problem. Consider, for example, the following statement:

Suppose somebody wants to buy information from American Express so they can send hate mail to the Mormons. Is there a point in the organization where the decision to sell is subjected to scrutiny? A lot of thought has to go into what you collect. . . . We avoid as many sensitive areas as possible. That’s why Buyer’s Choice initially decided to stay out of fund-raising—it’s controversial. But then fund-raising people started asking me to put these topics on. . . . When both sides wanted these topics included, we finally added questions on some charities to our survey. . . . [But we, like] most direct mailers place decoy names on every file they rent. It’s called a “seeding” in the industry. It ensures that a client won’t show us one letter and mail another. That’s how we can avoid the people who send hate mail to Mormons.
\textit{Id.} (quoting a Buyer’s Choice Executive).
\end{itemize}
Another problem is increased information search time. There is the problem of receiving ordinary commercial solicitations that are unwanted. Consumers have no control over the prospecting efforts that produce the bulk of mail they receive, and they are forced to sort through the mail. If you could see my dining room table sometimes, you might shudder. My dining room table becomes full of clutter and a lot of it is the result of this kind of aggregation and “merging and purging,” as they call it. The impact in individual cases is trivial, but the net effect on my ability to make informed choices may not be.

Yet another problem consists of nonconsensual government disclosure. The problem is that unregulated access to information which consumers have provided to obtain benefits from the government allows users to obtain these consumer’s names. You can buy a whole file of benefit data or driver’s license data and get all that information about people, including their height, weight and eye color. This type of information is in the public record and some states choose to sell it. At the current time, some people are being targeted for weight loss programs if their weight is disproportionate to their height.

In 1989, there was a famous episode in which the TV actress Rebecca Schaeffer was killed by a man who obtained her home address through the California Motor Vehicle records.

There are several alternative proposals for ameliorating the problems I have discussed. I suppose that the easiest and most persuasive, as far as many are concerned, is simply to do nothing and let the problems fade away. As we are reminded by some of the newer schools of legal analysis, we are wrong if we think that the only law enforcement mechanisms are in the hands of the govern-

29. Id.
30. Id. Additionally, without even knowing their name, people may be able to obtain a person’s address. Or, suppose that someone runs you off the road. If you run their plate through the system, you can get their name and driver’s license number, which in 26 states is their social security number. There is much that can be done with someone’s personal information, including getting a credit card in their name. Id.
31. Id.
ment. After all, there are other kinds of ways in which customs and practices are formed.

There are social forces which can be applied to discourage antisocial behavior on the Internet. I am told that in the electronic mail community, there is a lot of informal disapprobation that goes on. In other words, you can be the subject of a lot of "bad mouthing," if, indeed, you behave in a manner that is irresponsible.

Then there is also the more forceful way, the unplugging of Internet offenders by private agreement or by community vote. You can unplug an offender vertically if you have what is called a host-based system, and you can control the offender's access; or horizontally, if you control a network and are displeased with the conduct of a system, by denying interconnection to a network.53

So, in either case, there are these informal social mechanisms and agreement-based systems of control. Will self-regulation or reliance upon these "social forces" be sufficient?

The market-oriented argument against the regulation of the sale of information is that the problems of privacy and abuse on the Internet are self-correcting. This theory posits that the industry, in its desire to attract customers and avoid governmental regulation, is going to develop industry-wide standards to protect the profits that are being generated from this new technology.

If there is an abundance of fraud and a lack of privacy on the information superhighway, the argument is that consumers are not going to be willing to get on to it. It is going to cost money, it is new, many people are not comfortable with the technology, and if, in addition, it turns out that the information is going to be misused, people will refuse to get on it. Therefore, this argument goes, the industry will eventually be forced to police itself in order to encourage consumer use.

Apart from the willingness to tolerate what I would call distributional effects that are in all likelihood inequitable, this argument is to me more than a little bit hypothetical and long-run in its

expectations of success. It presumes that consumers have the necessary information about the problems that they are going to encounter and, accordingly, can make an informed choice at the time they do the contracting. It also presumes that even if consumers had the resources with which to make an informed choice to contract with a service provider, there wouldn't be a much larger social benefit to baselining standards within the entire industry. Finally, it also presumes that the industry is not more interested in the appearance of providing protection than in protection itself.

Consumer experiences in other related industries are not particularly comforting in this regard. At the recent 1994 meeting of the Direct Marketers Association, one analyst reported that fifty percent of the catalogers don't give their customers a convenient way to remove their names from a company list, which "does not bode well for the industry's claims of effective self-regulation."34

Even if all of the association's members complied with guidelines, there is no guarantee that the information brokers who provide this information and who provide the list are going to abide by the same standards. It appears that industry self-regulation provides inadequate protection for consumers, even when public and political attention is actually focused on the problem, let alone when it is not.

Another approach that we might consider is widely acceptable, and that is to increase the burden on consumers to look out for themselves. This attitude reminds me very much of a study I did about auto safety.35 When the automobile industry was young, the primary focus of preventing accidents (and there were a lot of accidents when the auto industry was young) was on what the wags began to call "the nut behind the steering wheel."36 The "nut" behind the steering wheel was usually the driver, who was supposed to be responsible for these accidents.

Today on the Internet we have a similar situation that is devel-

34. See Waldrop, supra note 22.
35. See SILBER, supra note 2, at 75.
36. Id. at 80; see also RALPH NADER, UNSAFE AT ANY SPEED: THE DESIGNED-IN DANGERS OF THE AMERICAN AUTOMOBILE 232-33 (1965).
oping with respect to consumers. In magazines and in newspapers we see lots of literature about what consumers can do to protect themselves. It also reminds me of the campaign for self-protection on the New York city subway—you know, you see signs like, "Watch your wallet!" as if that is the best response for you and the subway system to take to prevent pickpockets.

Well, in a similar fashion, consumers are being told that they can "adopt certain strategies to safeguard both their informational privacy and their right to be let alone." To avoid calls from telemarketers, consumers can use answering machines to screen their calls, or to prevent information from being gathered through credit cards, consumers can always use cash if they want. However, most consumers would agree that these are not satisfactory responses: answering machines eventually have to get listened to, and carrying cash can be inconvenient and dangerous. Of course, consumers who don't want the risk on the Internet can just get out altogether, but it is becoming more and more important and more and more necessary for all of us to use the Internet as a marketplace.

The service providers, I believe, take advantage of their bargaining power to shift burdens to their consumer members. A standard form agreement used by Delphi, for example, in its section on "representations, warranties and acknowledgements," requires that the consumer guarantee that none of the rights of others are going to be violated. Furthermore, the agreement informs consumers that "by submitting information or materials owned by you for publication or posting on, or distribution through Delphi Internet, you will be deemed to have granted Delphi Internet non-exclusive permission to redistribute by transmission the information or materials worldwide without charge or liability."

A member agrees not to "hold, seek to hold, Delphi Internet

38. See Delphi Membership Agreement, supra note 25.
39. Id.; see also Michael Noer, Policing Cyberspace, FORBES, Apr. 10, 1995, at 50.
liable for loss of data or misappropriation or infringement of any intellectual property right to which [the member] claim[s] ownership.\textsuperscript{40} By shifting liability to consumers, the Internet service providers avoid spending time or money to police their networks to minimize consumer fraud. The Delphi Internet membership agreement provides that members are entirely responsible for commercial services that they enter over the Internet. Here I will quote again from the Delphi agreement:

If ordering merchandise and/or services from anyone other than Delphi Internet, through any commercial services available, all transaction terms, including but not limited to purchase terms, payment terms, warranties, guarantees, maintenance and delivery are solely between you and the seller of the merchandise services. Delphi makes no warranties or representations whatsoever with regard to any goods or services provided by the seller of the merchandise or services and shall not be liable for the costs or damages arising either directly or indirectly from the products or services or from the actions or inactions of the seller.\textsuperscript{41}

As a result of the structure of the Internet, with its interlocking networks and agreements such as the one that I have just quoted, I believe that the Internet has accurately been called "the closest thing to anarchy that has ever existed."\textsuperscript{42}

I am not expert in the area of First Amendment law or privacy law; however, I believe that most of the efforts to reinvigorate privacy law so as to solve these problems will prove ill-fated. That is to say that the proper legal paradigm for promoting effective regulation of the Internet’s intrusiveness with respect to merchandising is not to resort to the privacy paradigms that are being debated in this Symposium.

\textsuperscript{40} Delphi Membership Agreement, supra note 25. The university or the corporation setting up the LAN or cluster of LANs is both the legislator and enforcer of rules on the Internet, but the boundaries between LANs blur as the communities intersect. Id.

\textsuperscript{41} Id.

\textsuperscript{42} Philip Elmer-Dewitt, Battle for the Soul of the Internet, TiME, July 25, 1994, at 50.
The central problem with the privacy paradigms is that "[t]he computers that process personal data for the information society . . . are located outside the individual space that is traditionally protected as private." Once computers record information about a person, this data can no longer be considered part of the private preserve of the data subject.

The creation of records that detail one's existence and way of life is a permanent condition of our society and, unfortunately, the privacy doctrines have not done much to serve that interest. Because the computer allows most of the innocuous information to be used in ways that are highly offensive to many individuals, both non-sensitive and sensitive data is going be inappropriately protected by privacy law.

And privacy analysis doesn't help determine how the law should permit personal data to be collected, processed, and used by others. As interpreted by the Court, the Fourth Amendment protects only those subjective expectations of privacy that the society is willing to accept as reasonable. Once society diminishes the expectations of reasonableness, as it has done in cyberspace, the Court has generally not been willing to restrict incursions into the private sphere. Even if the Court were to do that, its methodology which defines privacy in terms of physical area and information within that physical area, would still leave the Court to respond inadequately to consumer problems with respect to the computer.

What I would like to recommend is that we consider returning to the kind of analysis, statutory reform, and administrative en-

43. Schwartz, supra note 33, at 1346.
44. Id.
45. Id. at 1347.
46. Id. at 1345 (referring to California Bankers' Ass'n v. Shultz, 416 U.S. 21, 89 (1974)); see also U.S. CONST. amend. IV.
47. Schwartz, supra note 33, at 1345 n.32.
48. Id. at 1323 n.3. The professed goal of French data protection, for example, is to place "infomatics at the service of each citizen, insure its development within a context of international cooperation, and prevent it from damaging human identity, human rights, private life, individual rights, or private rights." Id. (citing Oliver v. United States, 466 U.S. 170, 177-82 (1984)).
forcement efforts that have been favored when consumers have challenged fraud and misrepresentation and oppressive contracts of adhesion in many other contexts.49

In a classically competitive free market, consumers exercise power by electing one provider or another according to their wishes and differences in the type of services available.50 But real markets, including, as we have seen, those on the Internet, are imperfect. Despite the number of those who are joining the Internet, the markets for selecting particular vendors and for selecting the privacy that you want are far from perfect. There are, no doubt, significant transaction costs in terms of time and money spent associated with searching for and changing to an alternative service provider.

There is no significant negotiation that takes place with retail consumers over the standard form contracts that contain the terms that I have talked about so far. Competition to provide higher degrees of privacy may be considerable when the buyers are banks or corporations, but not when they are most other folks. Furthermore, in a market environment, the transaction costs of finding a vendor that gives you more privacy or more protection from fraud may exceed the costs that are associated with either enforcing the laws against your current provider or switching over. This is particularly true when a network user "makes a significant investment in network specific software or hardware, in other words, when there is significant detrimental reliance on the network's service terms."51

I think that relational theories of contract—those which recognize the disparity in information and bargaining power between the parties, and which have provided a foundation for many consumer protection statutes and uniform laws and court-made laws in the past—offer a justification for relaxing the traditional contract law in coping with the realities of network communities. For example, there is a problem of network intermediaries who don’t have a

49. See, e.g., MICHAEL GREENFIELD, CONSUMER TRANSACTIONS (1992 ed.).
51. Id. at 357.
relationship to the originator, the person who signed the contract. Well, it seems to me that addressing this problem relates very much to the problem of privity in a conventional contract form, and that a rather straight-forward approach to the problem would be to strengthen the cause of action that people would have by relaxing a privity requirement.

With respect to fraud, the time-worn elements are still the same. The necessity is to educate consumers about the problem and to use legal rules to strengthen the rights of consumers to take actions against: (1) those who send them solicitations; (2) the vendors who provide sellers with the lists; (3) the list vendor's sources; and (4) the Internet service providers.

Through Federal or State consumer protection laws, various minimum standards directed to establishing minimal rights need to be grafted into the law. I have two which I will briefly suggest. One standard would be to create strict rules for consumer opt-outs and waivers, including opt-outs from Internet subscriber lists. Delphi, CompuServe, America Online and others allow subscribers to choose whether or not to be on mailing lists sold by them. This takes place after the consumer signs up and periodically thereafter. It is arguable that if consumers have signed up and have taken part in the service, and if once a year they have received the opportunity to opt-out but they haven't opted-out of such a list, then they have accepted the consequence of being on such a list.\(^5\)

The problem, from my point of view, however, is in the framing of the choices that the consumers are presented with: the deceptions, the limitations, and the unequal bargaining power.\(^5\) This problem can be addressed by adopting significant and sensitive consumer rules in this regard.

The fact that consumers want more choice in opting-out is clear

\(52.\) See Waldrop, supra note 22. American Express, for example, is proud of the fact that they allow customers to opt out of lists. \textit{Id.} It has a privacy council that meets regularly and reviews company policies. \textit{Id.} Every employee who gathers consumer information sits down and tells exactly what they have. \textit{Id.}

from looking at surveys that have been done by the Direct Marketing Association. Already some 2.9 million people have opted out of direct marketing offers. But such systems of universal opting out often eliminate categories that the consumer might want. What most consumers really mean when they do or don’t opt out is that there are certain things that they want and certain things that they don’t want. I agree with those who have developed “categorical” opt-outs which allow people to suppress certain categories of mail.

There is a group called Buyers Choice, which is a Division of Equifax, that collects data on the categories of mail that people want and don’t want. Out of one hundred categories, the average consumer is said to want only about forty. California is now the first state to actually require that credit card customers have the opportunity to get off of lists. If the lists are sold, the California cardholder has to be given “clear and conspicuous notice,” including a mailing address or a toll-free number for easy opt-out.

The second proposal that I would make for a minimum privacy standard is to restrict the ability of list purchasers to buy “sensitive” information about consumers over the Internet. In the United States there is no such thing as sensitive information except as people choose to define it themselves. Even the Standard Rate and Data Service mailing list catalogue, which is a standard industry tool, includes lists that reflect such sensitive information as sexual preference, religion, medical information and political contributions. But, according to list industry professionals, “you do have to sepa-

---

54. See Wilson, supra note 21.
55. Waldrop, supra note 22.
56. Id.
57. CAL. CIV. CODE § 1748.12 (West 1994).
58. See id.; see also Kenneth Howe, New Law on Credit Privacy, S.F. CHRON., June 30, 1994, at D1.

The credit card issuer shall provide a written notice to the cardholder that clearly and conspicuously describes the cardholder’s right to prohibit the disclosure . . . which discloses the cardholder’s identity. The notice shall include either a preprinted form by which the cardholder may exercise this right or shall advise the cardholder of a toll-free telephone number which the cardholder may call to satisfy this right.

Id.
rate sensitive and non-sensitive information. The solution for sen-
sitive data like medical or credit card records is regulation.59

It seems to me that legislative bodies may well find that certain
lists are generally used for purposes that the public doesn't wish to
permit, and therefore, should prohibit their transfer without explicit
consent by the individual consumer.60 Indeed, the Crime Control
Bill,61 which passed recently, contains a provision that makes driv-
er’s license and auto registration information essentially inaccessible
to individuals.62

There is a point at which each of us, I think, really believes
that the inquisitiveness of others ought to be unlawful. In the play
A Streetcar Named Desire, Tennessee Williams' character Blanche
Dubois says in closing, “I have always depended upon the kindness
of strangers.” Unfortunately, we can't be so trusting today.

PROF. REIDENBERG: Thank you, Norm. You presented
a very interesting take on commercial privacy; the notion that a
commercial transaction or the consumer’s involvement ought to
stop with the one-shot transaction, the buy or the sell. Your dou-
ble-edged view of anonymity—bad on the fraud side, but necessary
on the consumer side—I think is an important insight.

The next presentation offers a look at communications on a net-
work from a very different angle: in particular, the issue is how
we protect information where it is the government that is coming

59. Waldrop, supra note 22.
60. Oglivy and Mather recently developed a set of voluntary guidelines to encourage
responsible behavior by Internet marketers:
1. Intrusive e-mail is not welcome.
2. Internet consumer data is not for resale without express permission of the
   user.
3. Advertising is allowed only in designated newsgroups and list servers.
4. Promotions and direct selling is allowed but only under full disclosure.
5. Consumer research is only allowed with the consumer’s full consent.
6. Internet communications software must never hide concealed functions.
See Jane Weaver, Net Gain, INSIDE MEDIA, July 13, 1994, at 28.
62. But see Waldrop, supra note 22 (indicating that some press and First Amendment
scholars argue that there is a constitutional right of public access to such data).
in and getting access as opposed to, say, marketers buying and selling our personal information.

We will look at the question of what we can do to protect our information when the government may want access to it, and what we, as citizens engaged in network communications, can expect.

We will hear from Peter Drew Kennedy, who is a graduate of the University of Chicago Law School and Southwestern University. He has been very active in the litigation field and in computer communications. In particular, he was one of the attorneys in the case of *Steve Jackson Games*,\(^6\) which he will be discussing today.

MR. KENNEDY: I am going to do my best to keep my remarks fairly short today, for two reasons. One is that the topic of privacy is so broad, and I am going to be dealing with issues very different from what Norm did, so I would like to save time to answer questions and get into discussions, because it is interesting the way that these issues are sort of interlocked.

Second, because the law is so poorly defined as applied to this technology, it is difficult to say what the law is, but it is interesting to talk about what type of situations exist and what the law might be, or what decisions might be made depending on fact situations.

As I said this morning, my law firm and I got involved in computer communication issues through the back door. We were contacted to represent a small role-playing game company named Steve Jackson Games. I don’t know if you folks are familiar with the case, but they publish a series of role playing games called “Gurps.” It is a Generic Universal Role-Playing System, similar to “Dungeons & Dragons.” They published this game in book form, usually soft-bound books, and some hard-bound books as well.

In the late 1980s and up to 1990, as a service for their customers, they were providing electronic bulletin board systems. The folks who play role-playing games are fairly intense and it is a serious hobby. At Steve Jackson Games, they had a very well-

---

defined set of customers and game players that had set up this bulletin board system, but compared to the large commercial systems that we have been talking about today in the Internet and the different levels of Internet like the World Wide Web and Usenet, this was stone age technology. It ran on an XT computer; I think it had a forty meg hard drive, a single telephone line, and a single twenty-four hundred Baud modem at the time.

But in 1990 it was still fairly cutting edge to have this as a service. The board had several different areas in it. On the day that the Secret Service walked off with it, the board had about three hundred and sixty-five subscribers. It had an electronic mail system within the board so that all the subscribers could send private electronic messages to each other, and it had a series of bulletin board areas where the subscribers could leave public messages that could be read by other subscribers to the board where they could talk about their particular favorite role playing game.

The board also had a series of file areas, which was maintained by the company itself, where the company posted articles about game playing or articles of interest to game players. They also used the bulletin board to post draft games that they were writing. The company would post the drafts on the board and their best customers would download them and "play test" them to decide whether they liked the game and whether it worked well or not. Then the subscribers would provide input back to the company: for instance, they might say, "it would be better if these monsters had three heads instead of two." It was typical role-playing stuff, but it was a very valuable tool to the company to get that type of prepublication feedback from the customer. You will see that lots and lots of companies are doing this now, regardless of whether they are a high-tech or low-tech industry. They will have customer feedback through a customer support bulletin board system so that they can provide contact with their customers.

One of the advantages to this system is that there is no real-time connection necessary. A customer can dial up in the middle of the night and leave a question—how do you work this software, how do you work this toy, how do you work this game—and the company can reply back in due time through the private electronic
At the same time that Steve Jackson Games was publishing their games and running this bulletin board system, there was an investigation bubbling in Atlanta, Georgia concerning the illegal intrusion into a Bell South computer. Some hackers, namely teen-aged kids in Georgia, had gained unauthorized access to a Bell South computer and came up with a "trophy," which is essentially what most hackers do. They nose around systems they are not supposed to be on and they come up with a "trophy" which they can then show to their friends. They say, "look at this computer I got into, and this is a little trophy I got from it."

Well, the "trophy" that these teenagers came off with was a very bureaucratic document concerning the workings of the enhanced 911 system. It sounds scary, it deals with the emergency 911 system, but essentially this is a document which said who in the huge Bell hierarchy was in charge of what parts.

These hacker kids accessed the information and then stored it on another computer. Eventually it made its way to a fellow who published a little underground newsletter. He took this document, edited out a lot of the sensitive information, such as telephone numbers and things, and then again, as a trophy, published it through a large mailing list on the Internet as part of a newsletter.

So again, another reason to sign up for Usenet or Internet is so that you can get these things, because it is neat stuff that gets sent out. I subscribe to a digest called Computer Underground Digest and it is essentially a compilation sent out two or three times a week electronically with interesting articles that people pick up, stick them on there, and distribute.

There was a newsletter called Phrack which dealt with topics of interest to hackers. In one of the articles they had pared down this Bell South document which had originated in Georgia, and sent it out on the Internet to many people. The Bell South folks found out about it and weren't real happy. The three kids in Georgia eventually were indicted and pled guilty. The security folks in the Bell System started tracking the stuff down and they went to the Secret Service.
The Secret Service is responsible for, among other things, prosecuting fraudulent money and protective presence, and a variety of odds and ends of law enforcement things. One of their areas of jurisdiction is certain types of computer fraud and computer intrusion, which area they share with the FBI. The Secret Service is getting involved in doing this type of prosecution. But in this case, they were relying heavily on the private security forces of the Bell Companies, who were essentially coming up with articles and saying in effect, “Here are all the articles: go conduct a search.”

Bell South had tracked one of these Phrack issues with the edited Bell South document to Austin, Texas, which is my hometown, and they found it posted on a bulletin board system run by a fellow out of his home. He had a small computer and he and a friend ran this little bulletin board system as a hobby. Among all of the issues of Phrack that they had available on their bulletin board system for other people to come and download, was the issue that contained this edited version of the Bell South document, the “trophy.”

Security officers for Bell found this bulletin board system in Austin, Texas and they downloaded it and went to the Secret Service and said, look, we found it, one of these guys has got this document on this bulletin board system down in Austin, Texas. The Secret Service was also told that this person worked for a company called Steve Jackson Games, and that the company also ran a bulletin board system, Illuminati.

So, the Secret Service went down to Austin, Texas and got a search warrant and they busted both places. They went to this guy’s house and they took his computer and they went to Steve Jackson Games. Even though the Secret Service didn’t have any evidence that anything wrong was going on at Steve Jackson Games, the company was nonetheless running a bulletin board system, Illuminati. It didn’t have the Phrack document on it, nor did it have any evidence of any wrongdoing on it, nor any discus-

64. See id. A heavily-edited 911 document was available on a computer bulletin board system, “The Phoenix Project,” which was operated by Loyd Blankenship. Id. at 435.
sions about computer hacking. The only evidence was merely the connection between this employee and the company.

The Secret Service was unfamiliar with the technology, but went and got a search warrant from the Magistrate and at dawn on March 1, 1990, they were at the door of Steve Jackson Games, ready to take essentially anything with a computer chip in it. And they did. The Secret Service executed the search warrant and they took the bulletin board system, which ran twenty-four hours a day and was still up and running at the time. They took a broken computer; they took a computer from the employee’s desk; they took boxes of floppy disks; and they took printed copies of a draft book.

An interesting element of this, coincidentally, is that the company was about to publish a game book called *Gurps Cyberpunk* which was a role-playing game about computer hacking. You don’t use a computer to play, instead you sit around a table with dice and a book, and pretend you are computer hackers. There are also a bunch of rules in the book about pretending you’re a computer hacker. It was a role-playing game in the cyberpunk science fiction genre, which deals with folks who take their brains and plug them into computers and then go “surfing.” It had a bunch of realistic sounding information about computer hacking in it, but it wouldn’t do you any good if you were trying to do any computer hacking, unless you had a little port to jack into your head.

Nonetheless, the Secret Service got worked up about it. They seized the book, the computer and the bulletin board system, and the bulletin board system had the draft of this game on it because they were soliciting comments from their users about whether or not this would be a good game. Indeed this was a hot topic at the time and they thought this game was going to be a big seller.

The Secret Service carted off all the stuff to their Austin office. Steve Jackson arrived the next day and basically said, I need my stuff back, because we need to publish this book: we are a role-playing game company and you took all the copies of our book. But the Secret Service would not return any of the property. They gave him very limited access to the material and then proceeded to ship all of it up to Chicago where the computer experts were. It sat up in Chicago for month after month after month, and the com-
pany went through some very serious financial times. They laid off half their staff and had to reconstruct this book from very old drafts so as to finally get it out and publish it. Needless to say, they were very unhappy about what had happened at the hands of the Secret Service.

Steve Jackson tells the story better than I do, but his favorite part was when he went in on March 2 to the Secret Service and asked them to give his material back. His testimony was that the Secret Service agent had the draft of the Gurps Cyberpunk book and told him he was publishing a "handbook for computer crime," and that this was the directions for how to commit computer crime. And Steve Jackson was saying, well, no, really, this is just fiction, and you are not going to get anywhere trying to break into a computer using that book. But they saw it differently.

This incident raised a lot of questions in the computer community and raised a lot of sympathy. Steve Jackson was able to contact some civil libertarians and some very high quality civil liberties lawyers in Massachusetts and New York, and they filed a law suit on his behalf. They then brought my firm in as local counsel and eventually as trial counsel. The East Coast law firms stepped out for various reasons.

The difficult thing about the case conceptually was to figure out what laws were broken. What did the government do wrong? It was obvious to most involved that the Secret Service had bungled this fairly badly, had damaged a legitimate company and had invaded the privacy of a number of people. But the difficult thing conceptually is to figure out what they did wrong.

If you look at the initial complaint that was filed, it is a beautiful piece of work. I didn’t do it. It was done by a magnificent lawyer, Sharon Beckman of Silvergate & Good in Boston, and it sort of walks from the highest broadest principle down to the most lowly simple rule of law. It starts with the First Amendment and Fourth Amendment, works through a number of Federal statutes and it ends up, after we got involved, considering various state
privacy laws.65

The interesting thing about how the case worked out was a very difficult practical matter that we ended up dealing with. One of the reasons the case was brought was to try to establish that the constitutional principles of both the Fourth Amendment, which is a protection against searches and seizures, and of the First Amendment, the right of free speech and press, would apply in the electronic medium in the same way that they do in the print medium and in the broadcast medium.

One of the reasons behind bringing the case and suing the Secret Service was to try to recover damages for what had happened with the seizure. The difficult practical matter that we bumped our head against was the doctrine of qualified immunity.66 If you are all familiar with this from federal procedure or elsewhere, you, of course, cannot sue the government for violation of your constitutional rights, because they have not waived sovereign immunity. You can’t sue the United States and say, “United States, you have violated my First Amendment right and, therefore, you owe me money.” You have to sue the individual officers involved.67 The individual officers involved will be immune from suit unless you can show as a plaintiff that they violated a clearly established law.68 If you can show that they violated clearly established law,

---


66. The basic formulation of the doctrine is that an official performing discretionary functions has qualified immunity from damages liability under 42 U.S.C. § 1983 so long as his conduct conforms to a reasonableness test. Section 1983 states that:
Every person who, under color of any statute, ordinance, regulation, custom, or usage, of any State . . . subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured.

67. A state official may be deemed to have violated the Act if he knew or reasonably should have known that his conduct would violate the plaintiff’s constitutional rights or if he acted in bad faith. See, e.g., Scheuer v. Rhodes, 416 U.S. 232, 247-48 (1974) (“It is the existence of reasonable grounds for the belief formed at the time and in light of all the circumstances, coupled with good-faith belief, that affords a basis for qualified immunity of executive officers for acts performed in the course off official conduct”).

68. See, e.g., Bivens v. Six Unknown Named Agents, 403 U.S. 388 (1971) (where petitioner is granted monetary damages for injuries suffered as a result of search conduct-
then you can sue them in civil court and recover damages and establish a precedent.

The Catch-22 is that if you are suing to establish constitutional law in an area where there is no clearly established law, then it is very difficult to win the law suit, because you have to go in and say, well, Judge, this is a new area of law and we want to establish these First and Fourth Amendment principles and we want to blame these officers for it. The judge then says, well, if they were not clearly established at the time then the officers are not to blame, and so we won’t make any ruling that the law was clearly established on March 1, 1990. So, you get stuck in a Catch-22, and the law never gets decided. The problem with qualified immunity is that you have difficulty establishing new constitutional principles in law suits against government agents because the law never gets decided.

When this issue was raised by the government, (unfortunately, almost two years after the law suit was filed), we were faced with the decision of arguing the qualified immunity point and very likely losing it. Even if we were to win it, there would be a direct appeal to the Fifth Circuit and to United States Supreme Court from the decision denying qualified immunity. If we won it, the government could appeal, but if we lost it, we would be stuck until the end of the case and then we could take it up.

We made the tactical decision of looking harder at the non-constitutional remedies that were available, and I think very surprisingly to most of the folks I counsel in this area, the law is fairly well-established with respect to statutory protections that you have as a computer user, particularly as a computer publisher, from unwarranted invasion of privacy by the government.

I am going to touch on three of these statutory protections and then I will sit down and hopefully we can talk a little more about them later. The most interesting statute and most obscure one until now is called the First Amendment Privacy Protection Act of 1980.69 This law was passed by Congress in response to an egreg-
gious search and seizure of the Stanford Daily's offices. The Stanford Daily had covered a disturbance at the university. It was a protest that had turned violent. They had pictures of it, and the campus police wanted the pictures of the disturbance as evidence in criminal prosecutions against folks who were involved in the protest.

The police obtained a search warrant, went to the Stanford Daily, searched their offices, and came out with pictures and evidence of the crime that had allegedly taken place on campus. The Stanford Daily, of course, had done nothing but cover the story. They were not accused of having been involved in any criminal activity. The case went all the way to the Supreme Court, who said that the First Amendment does not increase the standard the government has to show to do a search and seizure; it is purely the Fourth Amendment that applies.\(^\text{70}\) There was no violation of the Stanford Daily's First Amendment rights, even though, of course, as journalists they felt highly violated that their news gathering had been compromised in order to advance a government prosecution.

So, in response, Congress passed a statute which protects publishers of information from searches and seizures if they are not the target of the investigation.\(^\text{71}\) It is not a very well known statute, it is not the best written statute, but it is clearly on the books. And a publisher is exactly what Steve Jackson Games was, if you read the statute.

Steve Jackson Games was both a publisher of books and a publisher of information through an electronic bulletin board system, and, as such, the company held material that was intended to be distributed to the public. And, pursuant to the Privacy Protection Act, publishers are protected from a search and seizure of evidence which they are holding to publish, even if they are going to do it for a bulletin board system.\(^\text{72}\)


\(^{72}\) The pertinent language in the Privacy Protection Act states that:

Notwithstanding any other law, it shall be unlawful for a government officer or employee, in connection with the investigation . . . of a criminal offense, to
And so we were able to establish the precedent—and although Judge Sparks, the trial judge, skirted the issue a bit, I think the implications of his opinion are fairly clear—that as an electronic bulletin board operator, if you are holding material on your computer that you are intending to publish and distribute to the public, then you are protected from a search and seizure by the government unless you are the subject of the criminal investigation.\(^3\) The government conceded that Steve Jackson Games was not the subject of a criminal investigation, that only an employee of theirs was, and that since there was no evidence of any criminal activity in their offices, they were protected by the Privacy Protection Act. The government, therefore, was liable for the damages that they had done in seizing the computers and the drafts of the book.\(^4\)

The second half of the case dealt with the protection of the private electronic communications on the board. We had to reconstruct the evidence through the computer files that had been returned by the Secret Service, but at the time that the Secret Service seized the Bulletin Board system, there were something like one hundred and fifty electronic mail messages on the board. Of course this is a small bulletin board system, but that sounds like a lot.

The Secret Service took it to Chicago and started the bulletin board system again. In Chicago, someone read all the electronic mail, A to Z, and then deleted it. It was all thrown out. The fascinating evidentiary question to work on was to get all the files together, so we brought in the person who wrote the software, Wayne Bell, and he made the determination that indeed that’s what was done.

None of the users on the Board were suspects in the criminal investigation, with the exception of the one fellow who was an

---

74. 816 F. Supp. at 441.
employee and ran a bulletin board out of his home. So, all of the users, except this one, had their private electronic mail read, analyzed and thrown out by the government without any probable cause that they had been involved in any violation of any law at all.

Most of the mail dealt with role-playing games and other such stuff. However, there were people who had struck up friendships because of their association and were exchanging private mail, and talking about private things. We had three of these users involved as plaintiffs in the law suits, and each indicated they had used this to send private communications and were highly offended by what the government did with their mail.75

The equivalent would be if they had gone into Steve Jackson games and found a stack of private mail that was sealed in an in box and said, “these are a hundred of Steve Jackson’s customers, I wonder what they are saying to one another, let’s read it and if it is not interesting, let’s throw it out.”

There is a federal statute which prohibits the government from doing this sort of thing.76 And it is encouraging that it has been construed to apply to this situation, because I am not entirely sure it was written for me.

In 1986, in an effort to catch up with some of the technology the Federal government passed what is known as the Electronic Communication Privacy Act.77 The Act added a new section to Title Eighteen, and it amended the Wiretap Act.78 The section the Act added to Title 18 is called the “stored access” or “access to stored computer communications,” and it essentially sets the boundaries for when computer operators can access electronic communications, when they can pass such communications to other people,

75. Id. at 439 (“Elizabeth McCoy, Walter Milliken and Steffan O’Sullivan also allege compensatory damages. These plaintiffs all had stored electronic communications, or E-mail, on the Illuminati bulletin board at the time of seizure. All three of these Plaintiffs testified that they had public and private communications in storage at the time of the seizure”).
and it set standards for government access to the electronic communications.\textsuperscript{79}

The Secret Service frankly admitted they really didn’t know about this statute and therefore had not attempted to stay within its guidelines. Additionally, the Secret Service and their lawyer admitted that they had never heard of the Privacy Protection Act of 1980. Didn’t know about it, didn’t know they weren’t allowed to kick open the doors in these rooms.

And I said, well, if it had been my client, the \textit{Austin American Statesmen}, which is a local daily in Austin, would you have done the same? And they said, yes, would have done the same. Which is a real frightening thing to hear from someone packing an Uzi while you are taking a deposition.

The third issue which we lost at the trial court and took up to the Fifth Circuit, was a twist on the Electronic Communications Privacy Act argument. The standard paradigm for electronic communication was e-mail. It is different than a phone call, in at least one way: it is not a real-time communication. You draft your electronic message, your e-mail, and send it to the attendant recipient. Even on the most simple system, like Steve Jackson Games, that mail will remain resident on the hard drive for a period of time before the person you send it to reads it.

I write an electronic mail message, containing something private, to a person. It is transmitted and it will be stored, at least temporarily, on a hard drive somewhere before the person to whom I have addressed it will have a chance to read it. It seemed that there were a number of messages like that on the board when Steve Jackson’s machine was seized. A lot of those messages were read and deleted as well. They were essentially en route to their destination.

The parties in the case felt these communications were especially sensitive. The person who had written the piece of mail no longer had control over it. The person to whom it was addressed couldn’t access it yet, hadn’t yet gotten a hold of the communica-

tion, but there it sat in a vulnerable state. And it was exactly at that point when the government stepped in and walked off with the messages.

We argued the seizure was an interception of an electronic communication, that it was essentially the same as a wiretap, because the government was placing themselves between the point of transmission and receipt of the message. The wiretap act was amended by the ECPA in 1986 to include electronic communications. Therefore, the government must follow the procedures necessary to wire tap a phone before it can intercept electronic communications such as computer communications.

In the situation of en route e-mail, we felt it was being intercepted in the same way a wiretap would have if they had tapped in and captured the data.

We lost this argument in front of Judge Sparks, and you can read the opinion for his justification. However, we won the other issues. Judge Sparks felt that the Privacy Protection Act had been violated and that the government had violated the historic Communications Act. The court awarded the company considerable damages for the loss experienced, and statutory damages for the violation of the individuals' e-mail.

We took the interception issue to the Fifth Circuit and we lost again. The Fifth Circuit said there is a difference: the Wiretap Act deals with contemporaneous seizures of transmissions and information as they pass through the wire, and the stored communication provision deals with e-mail that is sitting on a hard drive, regardless of whether it has been received or not.

I am not sure the Fifth Circuit is correct, and the government's position is defensible that the two acts treat the two things differ-

82. 816 F. Supp. at 441.
83. Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457 (5th Cir. 1994).
84. Id. at 461-62.
ently. If you ever try to read through the ECPA, you can see that it will support any number of different interpretations.

But it was an interesting and difficult issue to determine how these laws were going to deal with a very particularized fact situation where the technology falls somewhere in between what the two statutes seem to contemplate.

Well, I can beat a dead horse on this case all day, but I would welcome your questions on it, and I am going to just pass it on to the next panel member.

PROF. REIDENBERG: The case raises a very interesting juxtaposition. The privacy interests you were talking about, those of the company and those of the subscribers, versus the access to the information stored on the computer. And the purpose of the case was really to stake out the protection of content and the privacy of that. Unlike the consumer side, in this area, as against the government, you described a situation where there are some protections that are available.

Next, we are going to hear from Ronald Abramson. He will speak about a self-help mechanism, cryptography, and its role in the privacy debate.

Mr. Abramson is a graduate of Rutgers Law School and M.I.T. He has been very active in computer law and presently chairs the Association of the Bar of the City of New York Committee on Computer Law.

MR. ABRAMSON: My remarks are not going to be nearly as extensive as the other two speakers.

First of all, I would like to just make a few comments, after having listened to the other presentations. I guess the main one is that when discussing the Internet we have to, at least in my view, recognize what makes the Internet so interesting. Would this forum be as interesting as it is if all we had to talk about was America Online, CompuServe, Prodigy and Delphi? I don't really think so.

I think what makes this all so exciting is the fact that the Internet, first of all, is kind of spontaneous. It is something that developed out of military work, research grants and an academic
environment. So, it was there and it was essentially being subsidized while these phenomenal communication links were being set up, not just in the United States but worldwide.

Since no commercial interest was involved, nobody had planned this out in terms of whether they were going to make money. This was being done as a convenience to people who were doing research. It turned out they had a lot more capacity than needed, and it was realized that the Internet could be useful for a whole lot of other things.

The other thing that makes it interesting is the lack of regulation for the Internet. There really is no way to regulate it. I haven’t heard the word international yet, but that is what we are talking about. The Internet doesn’t have borders.

How many of you use the Internet? [A show of hands.] A pretty good percentage. I see also there are a number that don’t. When you get on the Internet and start sending messages, you realize that you don’t know where these messages are going, you don’t know what country the messages are going to. It is not uncommon to get on the service and see that some of the messages are in German, and some are in French. And chances are the people who typed all this German and French into the computer weren’t sitting in New Jersey. They were probably sitting in Europe. I have even seen Japanese characters actually on the screen. And these messages just bounce around on the Internet without regard to physical borders, which gives rise to some interesting phenomena.

For instance, if you take the situation where somebody wants to disguise their identity, either for good purposes or for bad; there are a number of ways you can accomplish that. One easy way is just to use a false identity when you sign up for a service provider.

Another way to conceal your identity is to use what is called an anonymous remailer, which is a service that allows you to send an electronic mail message repackaged under the remailer’s own header, stripping off yours completely. When that message shows up, as far as I know, there is no way to know where it came from.

If you use an anonymous remailer inside of the United States,
the information can be obtained through a subpoena. However, if you go ahead and use an anonymous remailer in Finland, recovery may not be as practical. I haven’t researched what is involved in trying to use the treaties to execute a warrant in Finland, but I bet it is pretty difficult. That is probably why the anonymous remailer in Finland is so popular.

Realistically, there is no way to control this stuff, and this is a fact of life. So, to the extent that laws are passed in the United States, to a great degree those laws would be ineffectual in dealing with a lot of these phenomena.

As I mentioned, the other thing that has complicated matters is the lack of regulation. People don’t want paternalistic services by and large. A lot of people feel comfortable with a protected environment such as America Online. However, a lot of people disavow that. They don’t want a protected environment. They want an Internet provider where you don’t sign an agreement.

There are a lot of Internet providers who do not require you to sign a written agreement. In fact, I know of an Internet provider that doesn’t even send you a bill. You send it money. If they don’t get your check payment, they simply turn off your account. There is no written agreement, there is no billing, there is no paper trail at all. They don’t have the ability, because they are not set up to do it. It is possible that they collect information on people, maybe they log every transaction that you do. They never signed anything saying they don’t. However, they also never signed anything exonerating themselves for such acts. Therefore, I doubt that they would engage in such behavior, because they would be exposing themselves to some considerable liability, absent a disclaimer.

But the fact is that this is a very prevalent type of service. I would suggest that, to some extent, if the system is going to thrive and fulfill its potential, it has to be left free in many of these regards. If you step in and regulate this thing, it is just going to wither and die or it is going to sprout up in some other way. People will find some other way to interact with it, where they are not regulated, because part of the attractiveness of the Internet is the freedom and the lack of regulation, and the fact that it is international.
In order to be responsive to Professor Reidenberg on the issue of cryptography, this is another issue where it is very easy to confuse the national and the international. I would suggest that we focus on the national and forget about the fact that there is a world out there.

One of the big issues in cryptography is the issue of export controls. Our committee just ran a seminar, a program at the City Bar, on the Clipper Chip. There is a transcript of that program that is available. It is quite interesting. The transcript is on the Internet, and if anybody is interested, I can give them the address where they can get the transcript electronically.

We had a very high level of debate. The panel consisted of people from the FBI, former general counsel of the National Security agency, an individual from the White House and the Director of Security at IBM, who presented a very broad and diverse view of the Clipper Chip and cryptography issues.

A very strong level of cryptography is available right now for free. It is called PGP, and it has a curious legal status. PGP is a system written by an individual named Phil Zimmerman, which combines public key cryptography and conventional cryptography. It uses public key cryptography, thus enabling a two-part key where you can distribute one key publicly and keep the other private.


In the mid-1970s, two Stanford University scientists (Whitfield Diffie and Martin Hellman) [invented] a new approach to cryptography known as public-key encryption. Diffie and Hellman developed a system with two mathematically related keys. Although the keys form a matched pair, it is computationally infeasible to derive one key from the other. Therefore, the system allows users to openly publish one key in a phone-book like directory (the "public key"), while keeping the other key private (the "private key"). Because the keys are mathematically related a message encrypted with one key can be decrypted by the other (and vice versa). In other words, each key is the inverse function of the other; what one does, the other can undo.

86. Cryptography generally is the process by which data is scrambled into an unreadable language in order to hide its content from everyone except its intended recipient. See id. at §§ 1-2.
I am not going to go into the details of export controls and cryptography, because I think enough has been written. Public key cryptography is very computer-intensive, relying heavily upon the computer CPU for processing. Instead of encrypting the entire message with the public key, you use the public key to encrypt a conventional key which is generated transparently on the fly.

The software creates a conventional key and encrypts the message, then it encrypts the conventional key with the public key and sends the message out. At the other end of the transmission the person who has the private key decrypts the internal conventional key—I don’t know if you are following this. There are two levels of encryption and the important part is that it uses the conventional cryptography for what it is good for, which is being very strong and efficient, while it uses the public key cryptography for what it is good for, which is providing the possibility of a two-way communication where you can distribute keys without having to worry about security.

The software works very well, and it is available on a number of platforms, PCs, Unix systems and Macs. You can download it for free. It is covered by patents, primarily the “RSA” patent, now held by Public Key Partners, the company that holds the patents on most public key cryptography right now. They have allowed this software to be used under license for noncommercial purposes. And, in fact, MIT took over the distribution and the authoritative version is available on an FTP server at MIT.

So, inside of the United States you can get this with the restriction that you not use it for commercial purposes. And if you want to use it for commercial purposes, there is a company called ViaCrypt, which has a license which they got a long time ago from RSA. ViaCrypt provides a license for $100 which allows you to use PGP commercially without concern about the RSA patents.

Since your license and these patents only exist in the United States and Canada, you are pretty well covered.

The only hitch is export controls. You are not allowed to export this technology out of the United States, which a lot of people consider to be a joke because anybody on the Internet can and does download this information. In fact, versions of this software were first released overseas.

One wonders how much sense this makes. Even during the cold war, people always wondered about export controls, whether they were effective or whether they were just crippling our industry. But one really wonders about it now, in an age where the cold war is over, particularly with regard to cryptography where the information is so obviously available all over the world. The opinion of many people is that the attempt to control exports accomplishes nothing against criminals and terrorists.

But certainly this is a tool that if you are interested in keeping your communications private, is legally available and used by a lot of people. It is a self-help security measure.

There are plenty of other self-help measures you can take. When Professor Silber talks about the junk mail, one of the things that people do is to throw it out. Or you can take measures like getting yourself off of lists. To take an example that is close to home, in my apartment building, we have two banks of mailboxes. In the middle there is a bulletin board and underneath that bulletin board there is a slot leading to a garbage pail. Literally, you go through your mail, take everything that looks like junk mail, and stick it in the slot. You don’t have to worry about dragging it upstairs or filling up your own garbage pail. Therefore, I don’t take much offense to junk mail, because I just throw it out. You are pretty close to the source. Additionally, when I sign off for things, if there is a space to opt out of having my name put on a mailing list, or having that mailing list sold, I check it. Basically I feel that a lot of these problems can take care of themselves.

The problem I feel won’t take care of itself is the situation where your information is involuntarily collected from you, and then that information is disseminated in ways over which you have
no control. These are the examples that were given before: the motor vehicle registry, the application for insurance, the application for a driver’s license, your use of a credit card. These are things that you really have to do every day and, by and large, you have to use your real identity, unless you want to start leading multiple existences, which I think would get a little weird.

This represents an area where you can’t really help yourself. You are at the mercy of the companies that are compiling this information, not only for purposes of sending you junk mail, which I think is fairly benign, but for other purposes. These other purposes include discrimination relating to employment, relating to insurance and so forth. I think substantial possibilities exist for this information to be misused.

The time is becoming ripe to really think about controlling how that information gets compiled and how that information gets used after it has been compiled. I think there are some really difficult problems of identification and definition here. You also have to be careful that any regime you establish does not start to restrict communications and itself become a burden on free communication.

But that is an area where I think that reform measures are really needed. I think that a lot should be done in terms of trying to define what the dangers are, what the abuses are and how we could specify laws that could control such dangers and abuses. Without reform, everybody’s personal lives will be more and more laid bare and be available for abuse. That is an area of great concern.

PROF. REIDENBERG: I would like now to open the floor to questions and then see where the discussion leads. I will exercise the moderator’s prerogative and start.

Several people on the panel have mentioned the need for consumer reform. Can the Panel address what law presently exists and what proposals are being developed to protect consumers and their information?

PROF. SILBER: I think California has taken a number of measures, and I think it is the leader at this point in creating an opt-out right with respect to credit card information. I also think I referred in my presentation to the Crime Bill, which has made
inaccessible certain driver's license information. So, there has been some work in this area.

I would like to respond to Ron's arguments against regulation. I am always a little bit skeptical when one argues against regulation based on its supposed futility. It is one thing to talk about the desirability of regulation as a matter of policy, but I question the historical argument that the world is too big, or that these people are too clever to be regulated; that we have anonymous mailboxes and we can't get to them, or we have to serve people in places like Finland. I concede that the problems are considerable, but I deny that they are insurmountable. As a way of illustrating what can be done if the will is there, I would point you to Article 4A of the Uniform Commercial Code, which concerns wire transfers, especially commercial electronic wire transfers of large amounts of money. Every day literally trillions of dollars of money is transferred from one country to another, not just to Finland but all over the world. And that is done, for the most part, securely and privately. It is done because of laws which are intricately designed to be state law, federal law, and, to some degree, international law.

Almost everybody likes anarchy until he or she is the victim of lawlessness. Fundamentally the issue becomes whether it is worth doing, not whether it is or is not futile. I am not suggesting that the task is easy. But I don't think that it does very much good for us to think about the problem as futile. I would suggest that we have a debate over concrete steps.

MR. ABRAMSON: Well, I don't want to dodge the question that has been asked and I think you raised some good points.

With respect to the issue you call "anarchy," I think that if you look at our legal history, a kind of laissez-faire approach pervades it in a lot of respects. If you look back at the 19th Century in terms of the laws that were passed as far as eminent domain and so forth, they are really set up to shield people from liability. And basically the reason was to let these industries grow, because this was perceived as a good thing.

I think there is a historical basis for that and I think it is a legitimate point of view. By the same reasoning, you could argue that when discussing companies like America Online or Delphi, with all the exculpatory language in their subscriber agreement, maybe there is some value to having our legal system recognize that it really doesn’t do any good to take somebody who is just serving as a carrier of information, as a medium, and make them liable for what boneheads happen to post on their system.

I don’t see the social utility that is served by making Prodigy liable when some idiot happens to post a message saying that somebody who runs a mutual fund is irresponsible, which is something actually going on right now.89

I don’t see the usefulness of having that level of regulation. In fact, I think it might be better to have a carefully crafted law that says Prodigy and other servers are immune from that kind of liability. Because Prodigy is not the real wrongdoer, and by assigning liability to Prodigy you are going to force them to start censoring. I think that would lead the law in a direction that a lot of people would rather not see it go.

MR. KENNEDY: I think we are dealing with two very distinct problems that Professor Silber raised. One is an area fairly subject to regulation and control, which is the collection by a service provider of personal information about the user when they sign up. In that situation you can identify who is responsible. The party gaining the information is an actor that you can say is responsible for its use of the information.

On the other hand, you are dealing with content regulations, trying to protect consumers from fraudulent transactions or fraudulent advertisements being sent through computer systems. The control of that is far more difficult and fraught with dangers to the service providers and to First Amendment values generally, because you are trying to control or hold people liable for the content of material they did not generate.

89. See discussion infra Panel I (remarks of Jacob Zamansky concerning the Stratton-Oakmont case).
The regulation of the collection and use of private information seems to be an area more susceptible to successful regulation. I have been "Internet-challenged" until fairly recently, and I think it is an observation from myself and from others that the optimism about the ability to successfully regulate the Internet is inversely proportionate to your contact with it. Folks who are most hopeful about regulating the Internet really haven't been on it, and the folks who have been on it for a while just kind of throw up their hands and say we are going to put a cap back on this Genie's bottle and get it back in.

The danger associated with collecting private information seems a ripe issue. In my experience in this area, there has not been a whole lot of attention directed to it, because the ability to collect that type of information through computers is staggering, especially by these computer services. They really have the ability of keeping track of all the purchases you make on the bulletin board. And with computer programs, they can sort information by type, taste, frequency and amount, as well as various other categories.

The need or the desire to control the use of that information is very valuable for the companies collecting it, and therefore it is an issue that really does need to be addressed more than it has been. It seems, up until now, that any abuse in this area has been worked out through informal pressure asserted on the commercial bulletin board systems by users when they found it out. For example, I think CompuServe has significantly changed over the last few years with respect to the way it uses that type of information and the amount of disclosure.

Another consideration is the very intense degree of competition among the commercial providers. I wouldn't want to under-emphasize the value of that competition in holding down the improper use of collected information. There is huge pressure and competition among these service providers for customers. I have bounced back and forth among commercial providers very quickly and it is not that hard to decide that if I don't like Prodigy, I can go to CompuServe, who don't regulate, and it will take me twenty minutes to change my account.

PROF. REIDENBERG: That may work for content, but for the
circulation of the personal information, it really doesn’t work. I may have a contract with a service provider that sets out terms for what they collect. That is well and good, but if I use that service provider to access any other Internet services, by necessity information about me has to get passed on to any node that my communication crosses through on the Internet. So, any node that I go through in getting to my Internet destination is now gaining a tremendous amount of transaction information about me.

The nodes may get my identity, they may collect information about the service I accessed, what I looked at, how long I was connected. All of those different pieces of address information and usage information are now going to be in various switches along the way.

It is sort of like the “Ernestine” sketches by Lilly Tomlin. The switch has the information: I am coming from Point A and I am going to Point B, and these are the key strokes that I am entering while I am doing it. The system can store it, whether it is actually being done or not, will depend on the network node.

Most people are probably unaware that all of their phone calls are profiled and, thus, in a sense monitored by the phone company. The original draft of the Electronic Communication Privacy Act would have restricted the phone companies from allowing transaction information to be disclosed, either to the government or to the private sector. The final version kept the restraints on the government, so if the government wants to know who you called, how long you were on the phone, they need to get a warrant.

On the other hand, it is perfectly legal for the phone company to disclose all your calling patterns to anyone else. The telephone company cannot disclose the contents of what you have said, but they can disclose who you called, when you called them, or anything else like that.

If you have ever dialed an 800 number and received one of the push button menus for various services or information, the call is not anonymous; they are getting your identity when you make that 800 call. Most of those systems will track what services you select. There is a whole audit trail.
There is really very little regulation in this area. There are some rules at the state level on Caller ID, and the requirements for allowing call blocking and call-screening features. There has been some Federal legislation proposed to restrict marketing uses of information collected through interactive communications. There are one or two state laws that impose limitations. But there is really very little in the United States.

To underscore, at least part of Ron’s point, this is a global phenomenon. However, I would disagree with Ron in his comment that regulation would simply fetter the development of the global information infrastructure or the NII, depending on which way you want to look at it. In fact, I would say precisely the opposite. Unless we start dealing with some kind of regulation on the fair uses of information on network systems, there will be a lack of development, because both business and citizens are not going to have confidence. 90

There is, at least in the United States, some recent polling data, coming out of the Harris organization, that supports this proposition. But I think more importantly, in foreign countries, they are addressing the privacy issue through very comprehensive legislation that will block data flows to the United States if we do not achieve something similar.

PROF. SILBER: Let me wind down this discussion of our future electronic consumer problems on a lighter note: there is an AT&T ad that many of you may have seen. It begins by inquiring, “Have you ever paid a toll without slowing down?” You see the car going through the toll booth, and there is a voice-over that says, you will. And then have you ever opened a door with your voice? And there is a voice that says: “You will.”

Shortly afterwards, on the Internet there was a list which parodied that commercial. Some of the line substitutes were: “Have you ever been pulled over by the highway patrol because the electronic toll booth checked your vehicle ID against a nationwide list

of parking tickets?" "You will." "Have you ever been locked out of your apartment because you had laryngitis?" "You will." "Have you ever received a phone call from your health insurance company telling you that they are cancelling your coverage because a scan of your supermarket buying patterns showed that you ate too much beef?" "You will."

There is an interesting problem here for consumers. The problem, as Professor Reidenberg says, is that the question of privacy cuts two different ways. On one hand we consumers value our privacy for a personal conversation. On the other hand, when there is too much privacy, then we consumers are victims ourselves of the fact that nobody is monitoring what is going on.

There is considerable tension here. The tension hasn't been resolved adequately. There is in fact a spectrum of privacy interests and it is not a matter that we can afford to be absolutist about if we are going to try and develop the right kind of regulatory mix.

QUESTION: If we are trying to set up a regulatory framework, given the invention of Caller ID, is there the technology to do this type of thing on the Internet, set up some kind of privacy detection? Because NYNEX just found out that a few hundred thousand people that opted for Caller ID blocking weren't getting it. So, is there some kind of way we can do this technologically to set up some systems that would protect privacy within the Information Superhighway, or are there going to be glitches in the system constantly, is it going to bypass, or is there some way to get around the problem?

PROF. REIDENBERG: Technological solutions may establish some privacy, but glitches will certainly be likely. What level of glitches in the system one is willing to accept is obviously critical. At least in NYNEX's situation, NYNEX was advised of the problems, but did nothing for a significant period of time. When NYNEX went to the New York State Public Utilities Commission to get authorization in order to be able to provide the Caller ID service, they were only going to propose, I believe it was per-call blocking. Per-call blocking would require dialing a three-digit code and then that particular call will not identify you. Instead, New York required NYNEX to offer customers per-line blocking, which
meant, if you were a subscriber, you could have NYNEX block identification for every outgoing call.

The PUC required NYNEX to offer per-line blocking as a condition of being permitted to offer the service. So NYNEX then went out and, of course, charged fees for the service. NYNEX was later advised that, in fact, it had not implemented per-line blocking on a significant percentage of their lines.

One of the NYNEX statements at the time was that if NYNEX had to offer per-line blocking, the service would not be viable because too many people would not want to be identified. Well, if that is true, that tells you something about how people value their privacy and suggest something very important about whether it is appropriate or not to offer per-line blocking.

Whether it was a glitch, an intentional act, or intentional negligence on NYNEX's part will probably be determined both by the PUC and by some courts resolving contract claims that are brought against the company.

In terms of technical capability on the Internet, you could structure systems to have an equivalent pro-privacy capability. For instance, as Mr. Abramson pointed out, when sending e-mail you may strip your identity by using an anonymous remailer. That is the equivalent of call blocking on Caller ID.

Similarly, with video dial tone or the cable service, you can structure the network so that if marketing information is stripped of your name. The system may capture the date and may aggregate data, but not specific data. There are all sorts of ways to do it.

MR. ABRAMSON: With respect to the other half of the question, you are asking four lawyers, rather than four technicians, about what can be done. And we are way behind the curve figuring out. And my experience is that almost anything can be done by these guys who "twig" with the computers. It is just absolutely amazing ability. We, as lawyers, respond to the technology once it is created. It is the technicians who actually develop these new "playing fields." Once the new "fields" exist, the issue then becomes, what we can do about them.
MR. KENNEDY: That actually is a point I wanted to make about fraud, because both of you have suggested that with respect to fraud we are in a different area than we are with respect to marketing. My argument would be that we need to think about how we can provide incentives to diminish the amount of fraud on the Internet.

MR. ABRAMSON: I think marketing has been taken down to a very low level in this country. My own feeling is that the Federal Trade Commission just dropped the ball during the 1980s, and you started to get this proliferation of absolute frauds, such as the junk about contests you get in the mail.

If you go ahead and play these things, you will see that a lot of them are frauds. These operators move from state to state because they usually attract the attention of the attorney general in one state. They simply wait until it has gotten too hot in Oregon, and move over to Idaho and then they move from Idaho to Nevada. Nevada is a pretty good place—you can get away with a lot in Nevada.

There is not that much enforcement at the Federal level in terms of what is deceptive and what is not. I think people have to come to accept that and people who are halfway intelligent now realize the stuff that you get in your mailbox cannot be relied upon. Certainly, other examples exist. For instance, whenever you hear an ad on TV, there is the small print on the bottom, which you cannot read. Or you hear an ad on the radio and again somebody starts jabbering at about 400 words a minute, and you can’t understand any of that for about three seconds. All these disclaimers are usually just enough to tell you, hey, there is a catch to this, don’t take it seriously.

So, I think it is possible to get overly concerned about some of this. There are some legitimate areas of concern, where, for better or worse, people will have to look out for themselves.

PROF. SILBER: I have a prediction to make. At some level, fairly soon, some state court judge is going to declare one of those adhesive contract provisions in one of the service provider agreements unenforceable, because it is unconscionable or overbroad or
for some good other reason. And at that point there will be some serious consideration given by the service providers to formulating standardized loss allocation rules that are more equitable. And then we may just discover a more effective way of dealing with fraud on the Internet.

QUESTION: I have a question for Mr. Kennedy. You mentioned the case you worked on concerning the prohibitions on reading e-mail, and you used the analogy of opening a sealed envelope. I work in higher education and we are working on problems with the systems operating in universities and colleges with e-mail, when employees have quit or mail has been misdirected. I have heard people say that e-mail is not sealed. Is there any law?

MR. KENNEDY: That is a question much easier asked then answered, unfortunately. I have spent a good bit of time talking with people like yourself, who are involved with providing communication systems. The confusion is attributed to how poorly written the statute is. Ed Cavazos, who has written the most recent book about cyberspace and the law, is a friend of mine in Texas, and his opinion is that the ECPA prohibits service providers from reading electronic mail that pass through the machine except in particular circumstances.

Jonathan Wallace, who wrote the earlier book on the same topic, has a diametrically-opposed position. He thinks there is an exception in the ECPA which allows service providers to read electronic mail, but not to disclose to anyone. Wallace believes that they have an exception where they can monitor the mail and pass it through. I side with Ed, and I have written a few articles saying that the better practice for people who provide these services, is not to read electronic mail, except in particular circumstances. One of the circumstances being to read enough of the mail to know what to do with it in your type of situation.

So, if you have someone who has left and no longer has the

---

92. Id. at 20-26.
94. Id. at 30-34.
account, you can read enough in the mail to forward it, for example. You can always read enough of a message to forward it to the next address or to figure out what to do with the mail.

Usually, if you are in that situation, you can do things that make sense. We use the "grandmother rule" a lot in Texas: if you can explain it to your grandmother with a straight face as to why you did it, and you think she will buy it without looking at you and saying, "Now, son," then you are probably on fairly safe ground.

Ed's book is called *Cyberspace and the Law*. It is published by MIT press. Prof. Reidenberg ECPA is a pretty tricky statute and it makes distinctions here. Specifically, there are distinctions about whether the message is internal to the system or whether it is going out to another system. Also the exceptions are written in a way such that I don't know if anybody really understands the scope. One of the exceptions, as I recall, is that the operators are allowed to go into these messages if it is necessary to protect the system. I think that is a hard standard to interpret.

The other side is a practical matter. When you send an electronic mail message, if you address that message incorrectly, then it is going to end up in some place where you never intended it to end up, and that's pretty easy to do. No one has committed any wrongdoing but the security of your message is totally compromised.

The situation is also complicated by the fact that ECPA is not the only applicable law. Most states have wiretap statutes, and a number of the states have wiretap statutes that require what is called "two party consent," which is both parties to the communication have to consent for disclosure to a third party. In that instance, the sender as well as the university employee would both have to consent to the university's reading of the message, if the university is treated as a third party.

There have been a couple of state court cases where the employer has been allowed to read the e-mail messages without liability.\footnote{See Scott Dean, *E-Mail Forces Companies to Grapple With Privacy Issues*, CORP.}
There is also an organization in Washington now called the Electronic Messaging Association that did a study of electronic privacy going back about three, perhaps four years ago written by David Johnson and John Podesta.\footnote{David Johnson was a lawyer in Washington, presently the CEO of Lexis Counsel Connect. John Podesta is one of the key staffers in the drafting of the Electronic Communications Privacy Act and is presently the staff secretary at the White House.}

They looked at this question as to what employer policies ought to do in light of both ambiguities and difficulties in applying the ECPA, particularly where the ECPA, as Ron just said, is going to depend on the circumstances. If the e-mail message is coming from a public carrier, that has one set of implications. If the message was strictly internal to the school’s LAN and it was never passed by a public communication service, then it may be treated quite differently.

QUESTION: The 1986 statute does outlaw the reading of electronic mail. The problem is not enforceable in the Internet.

PROF. REIDENBERG: The question is whether the ECPA authorizes the employer to read any employee’s e-mail?

I think that is still a very open question because many employers do not explicitly require that every use of the employer’s computer system be for work. For example, I know one of the major banks in New York has a global telecommunications network and they made it an expressed policy decision not to restrict the use of that network to business-related purposes, because one of the things they wanted to engender was a sense of community among the different offices all over the world.

One of the striking things for them was the volume of messages that were not business related between employees in their various branch offices all around the world. I think there have certainly

\begin{footnotesize}

\footnote{96. DAVID JOHNSON \& JOHN PODESTA, ACCESS TO AND USE AND DISCLOSURE OF ELECTRONIC MAIL ON COMPANY COMPUTER SYSTEMS, (EMA: 1991).}
\end{footnotesize}
been some courts that have taken the position that the employer can read anything. However, those were state courts, and it is not at all clear that that is going to be a widely held view under the ECPA, and it would also depend on the circumstances.

Again, it is a very narrowly drawn statute with respect to application and given the multiplicity of contexts, it is very difficult to say generically this is what would happen in a given case.

MR. ABRAMSON: A lot of attorneys routinely advise their clients now that they should have the employees actually sign waivers of confidentiality as far as the company’s e-mail system is concerned, and I don’t know what you may think of that, but under the current regime it is probably advisable for an employer. I think you will see more and more of that being done as people think about the problem. It is just another area where privacy concerns come up.

MR. REIDENBERG: Perhaps a final word to close. The ECPA has an interesting provision, which I think should terrify us as lawyers. The provision says that the system administration, for systems administration purposes, can essentially do anything. It is perfectly legitimate for a systems administrator to read all e-mail messages for those purposes. The reason I think that should terrify us as lawyers is that instead of setting up the lawyers as king, it sets up the SYS-OPs as king on the information highways.

Well, thank you all very much.