There are many arguments about what keeps people from using the Net -- and some sentiment, ours included, that things are moving along fine, thank you. People are moving onto the Net as fast as they can be expected to. Yet it's clear that many people, both potential users and potential government regulators, misperceive the Net as a scary, unregulated place. That misperception is likely to keep people away -- and to bring outside regulators in. This issue of Release 1.0 is the story of two efforts to forestall government regulation through a better solution: self-regulation.

Self-regulation is worthwhile both in itself and as a way to avoid government regulation. It is likely to be more flexible, more decentralized and more responsive to actual conditions than government regulation. It will foster maximum user choice, while at the same time breeding confidence among users that they can trust the medium. The goal is not to regulate cyberspace as a whole, nor to solve all problems concerning privacy or offensive content, but to carve out enough clean, well-lighted territory that the rest loses its power to scare people away. In the end, most people will prefer the safe neighborhoods, and potential predators will find few victims other than their own kind. For this to happen, we need strict rules on disclosure, and flexibility on most other matters.

In our December issue we discussed the use of labels for content control; in this issue we discuss their application to privacy. In both issues, we also offer a broader context: The value of labels is that people can pick rules that suit them, rather than be forced to operate in a one-size-fits-all environment where everyone has to follow the same rules. Obviously, that works only when one person's selection of rules doesn't impinge on another's -- precisely the case both in content control/filtering and in privacy. Each person can select the rules or content she prefers for herself or for her children or pupils. The basic rule is that providers must disclose -- label -- themselves clearly and honestly. And they must do what they promise to.

Unfortunately, the major challenge in privacy comes once personal data leaves any particular Web site. Nonetheless, even dealing with privacy as a local problem should go a long way towards encouraging consumer comfort -- and use of the Net. Making it self-regulated instead of controlled by the...
government is the goal of eTRUST and the Internet Privacy Working Group (IPWG), the pioneer privacy-labeling efforts we discuss in this issue. (In the interests of openness, we must disclose right here that eTRUST is a joint project of CommerceNet and the non-profit Electronic Frontier Foundation, chaired by Esther Dyson. We hope we can be objective about this effort, while firmly supporting its goals.)

The underlying question faced by eTRUST and IPWG is whether they can successfully garner industry support without the heavy threat of government regulation behind them. In short, can they raise the issue’s visibility enough to get the public to care about it and Websites to self-regulate but still not provoke a government-mandated/controlled system?

The goal is a market in privacy practices. That will result in constantly improving standards rather than rigid ones set by law, and in decentralized, speedy enforcement.

**Compare & contrast: content vs. privacy**

As described in Release 1.0, 12-96, rating content is relatively easy for third parties: All they have to do is look at what's on a site and rate it according to their published criteria. Different organizations or individuals with different criteria can rate a site differently, and the site-owner can also generate ratings. Ratings can be either subjective and prescriptive, or more factual, concerning the presence of certain kinds of material. Checking the ratings is easy; observers can tell right away whether it has been accurately rated (whether or not they agree with the criteria used).

By contrast, you cannot tell much about privacy or security by looking at a site; privacy and security are dependent on processes which may not be visible to outsiders -- and may be too complex to rate easily. (Yes, we could imagine a service that rated news sources according to their fact-checking practices, but let's ignore that for now.) The details need to be specified. "No data is kept" is easy. But "certain data are transferred to others" is complex: to whom? under what conditions? and so forth. If there is a problem, you may find out the awful truth only when it's too late.

Moreover, though content is the same for all comers, rules concerning privacy may apply differently to different customers, at the site's or the customer's option. In the simple model, each Website may have a blanket policy about data re-use, and customers decide whether or not to interact with it. But a Website may instead offer a number of options, and customers can negotiate -- perhaps paying in anonymous e-cash to see something that would be free to an identified viewer, or providing specific personal information in exchange for a discount or customized service.

---

1 Yes, there are instances of clean and dirty versions of games or movies, or different-language versions. Blind people may rely on captions for graphical content, which also render the content easily searchable -- and classifiable. Moreover, sites can deliver content selectively according to their knowledge of individuals, but that slips into those privacy discussions again!
In considering rules for privacy, one must distinguish between prototypical consumers, whose only behavior is to take something offered and perhaps pay for it with cash, and producers or fiduciaries, those who promise to do something: offer a safe and effective product, fulfill a credit agreement, care for children or hold a public office.

Here we are concerned with the privacy of individuals and consumers, concerning data in which society overall has no compelling interest. (Yes, access to customer information helps commerce along, but that's not what we mean.) Commercial consumer privacy is quite a simple moral issue, we believe: Customers should be able to choose what information to reveal and how it may be used, although they may have to give up some privileges to do so. Businesses can compete to satisfy those consumer demands; they are negotiable. In some sense, the passive "consumer" becomes an empowered "customer," able to specify what he wants, instead of selecting from a limited set of options. In the past, it was difficult for customers to specify and for vendors to observe such detailed conditions or receive detailed feedback; now it's fairly easy. It is also a fairly simple technical task to handle commercial consumer privacy with new data-management technology.

This issue of Release 1.0 deals only with consumer privacy and how to manage it -- or rather, how to manage the data associated with it. Weighing the trade-offs between privacy and society's right to know in other spheres is a far more difficult, non-technical question.

What is left out

Many requests for personal information are different from the commercial situations referred to above: They involve some coercion (more than just, "You can buy this sweater at a discount if you reveal your favorite color") or a potential breach of trust. For example, you may have to reveal certain information to get insurance coverage... and worse, the truth may de facto deny you affordable coverage. Children may be lured into revealing information that their parents would not allow them to. An employer may want to know about your criminal record. On the other hand, society has an interest in the truth of the information people do reveal -- no fair lying to the insurance company, or claiming a high level of income to get a loan.

Moreover, society has an interest in disclosure of information ranging from criminal records to safety risks. How bad a risk is a former drug abuser or an abusive spouse? Is the risk only to the company, to people who might be in the path of the truck that person is driving or to other employees who might provoke the person's wrath? We also have an interest in disclosure by politicians and other officials well beyond what we should require from private individuals.

All these situations inherently cannot be fairly negotiated. Governments do need to provide rules for using such information as appropriate and otherwise keeping it private securely and consistently.
But right now, a customer can't easily express his privacy preferences: He may have one preference for a site dealing with computer-industry issues, and another for his neighborhood after-school chat. We present different faces at work, at school, at church or temple, at the doctor's office (see Release 1.0, 4-96). The difficulty is that information changes character as it travels, in a way that "content" does not. Likewise, your concerns for security may depend on the kind of interaction you are having: Are you simply revealing your name, or are you transferring cash, or revealing deep dark secrets? Of course, right now you can refuse to supply any data, but greater granularity would be beneficial to both sides.

So what is needed? A way for both sides to express themselves, and some way to ensure that they are telling the truth. In practice, that means self-rating and honest disclosure, along with third-party verification to ensure honesty on one side and trust on the other. Such verification has another benefit: the spread of best practices via firms that specialize in privacy and security methodologies.

**Privacy as an assignable right**

The ideal solution for commercial consumer privacy is to rely on market principles rather than blanket regulation. As background, consider the work of economist Ronald Coase, who won the Nobel Prize for this insight among others. If you establish a right -- whether it's for clean air, privacy, a pound of potatoes or a copy of a newsletter -- that right will be allocated efficiently in a free market, regardless to whom the right is initially assigned. The issue isn't who owns it, but to whom it is worth more. That is, the market looks at the difference between the two sides' preferences, and the right goes to whoever values it more; a corresponding amount of value may change hands in the opposite direction.

In the context of privacy, the first question is whether Alice values her right to privacy more than WonderWidgets values the right to call her at home at 9 pm. If she does, she will effectively pay WonderWidgets for her privacy by forgoing the opportunity to receive a fee from the company. On the other hand, if she values her privacy less, she may sell the privacy -- the right to call her -- to WonderWidgets for that amount.

**Defining "privacy"**

But unfortunately those rights are not clearly defined. Second, they don't map easily to the pieces of data that we take to represent them: How does Alice distinguish between the right not to be called at 8 pm and the right not to be called at 9 pm -- although they're based on the same telephone number? How does she control the proliferation of those rights (de facto, information) into the hands of others who might use it differently? Does she need separate contracts with all the people who might possibly telephone

---

2 The issue of who owns rights (and other assets), and who can afford to keep and exercise them rather than sell or exchange them, is one of social justice, which is not our concern here. The only point to make here is that if rights are too concentrated, their owners may not use them properly -- and the outcome will certainly be unfair.
her? The market works well with defined items, less well with slippery pieces of data that change value as they get combined or change hands. Is the right to the piece of data, or to particular uses of it?

Indeed, when we say "privacy" we mean lots of things -- everything from the (non)publication of information to control over exactly when one receives a telephone call. Does Juan mind if his information is in a data bank somewhere, unseen by prying eyes? No. But he goes ballistic if he gets called after 7 pm. Alice, by contrast, gets the willies when she thinks of her transactions being recorded anywhere and seen by others, but she doesn't really mind the phone calls as long as the callers don't seem to know much about her. One doesn't want to be disturbed; the other is specifically concerned about privacy as an information issue.

Different people have different preferences for their own privacy.3 Any of these preferences is fine -- as long as it's clear what the rules are. The point here is that each Website should cater to the specific preferences of its users, rather than all following the same rules. Some people object in principle to the concept of privacy as an assignable right -- one that can be sold or bargained away. They'd rather see it as an inalienable right, one the poor can enjoy as fully as the rich. But our principles tend towards maximum personal freedom -- that people should decide for themselves how to value their rights. Since privacy is not an absolute, and since individuals' preferences vary, it seems foolish to insist on an absolute approach.

---

3 There are already many laws concerning privacy. In the United States, information about individuals' video purchases is protected -- the result of one unfortunate experience by one legislator that resulted in the law. On the other hand, data linking a person's driver's license number with name, address, age and other personal data is available from Departments of Motor Vehicles in many states. Much commercial data is more carefully protected, but often more for commercial reasons than out of respect for the privacy of the individuals concerned. By contrast, the European Commission places strong controls on the use of personal data, to the extent that many companies find it difficult to do business across borders; they can't even transfer data about their own employees from one country to another. That may be why direct marketing isn't doing so well in Europe, says Pat Faley, vice president of consumer affairs for the Direct Marketing Association.
Fortunately, there are several systems in the works not for privacy regulation, but for privacy disclosure and the labeling of data-management practices. Also, many Websites also have specific, disclosed privacy policies. It is up to the customer to decide on the value of his data and to act accordingly.

Like content labeling, these systems are contractual. They can work without any changes in existing law. The initiatives described are grass-roots, and they are designed to foster a multiplicity of approaches to privacy management, rather than a Central Bureau of Privacy Protection.

The first is eTRUST, a labeling and certification program sponsored by the EFF and CommerceNet of California. eTRUST is in pilot operations currently.

The second, complementary effort is in an even earlier stage; it is the Internet Privacy Working Group (IPWG), a coalition of about 15 companies and organizations convened by Washington's Center for Democracy and Technology. The IPWG is working with the World Wide Web Consortium trying to figure out how to extend the PICS content labeling protocol (see Release 1.0, 12-96) to the electronic labeling of privacy/data practices in a way that would allow automatic negotiation between a person's browser or agent, and the privacy rules of a Website.

eTRUST is a labeling system with three gradations, along with local rules specific to a site underlying the gradations. The IPWG’s P3 (for Platform for Privacy Preferences) will be more granular, and will enable a way of representing specific privacy rules in computer-readable form. The combination of eTRUST’s approach to labeling and certification, and the IPWG’s approach to representation and automatic negotiation, could end up as a powerful advance in Net civilization.

eTRUST

Since work started last year, the eTRUST partnership has been busy rounding up sponsors/partners who will help to cover the start-up costs of the free-to-users pilot program. (Even before eTRUST, there was a group with similar concerns but less coherence called Privacy Assured. Most of its members simply moved their support into eTRUST.) Participants in the pilot, with various kinds of involvement, include InfoSeek, WorldPages, Firefly, EUnet, Fourll, Quarterdeck, CMG Direct Interactive, InterMind, Narrowline, Portland Software, TestDrive, Britnet, Perot Systems, USWeb, Switchboard, the Boston Consulting Group, and a variety of other organizations, commercial and otherwise. Two leading accounting firms are also involved in helping to design the program and in validating Websites' privacy claims: Coopers & Lybrand and KPMG.

How it works

Privacy ratings differ from content ratings in that reliable outside rating (without the site's cooperation) is almost impossible and self-rating requires third-party attestation; privacy management is an internal matter, unlike content which is visible to outsiders. That's why the concept behind

Release 1.0 19 February 1997
might be willing to trust many different content raters, since he can assess them for himself and the dangers of a misrated item are low, but he's going to want a trusted brand name to guarantee his privacy. Over time, we hope there will be many privacy auditors, and some competition for eTRUST itself -- which after all is only a specialized kind of rating service. The more the merrier!

To post the Trustmarks on its Website, the site has to execute a contract with eTRUST, undergo an audit with an eTRUST-approved auditing firm, and agree to certain conditions.

The three levels of the Trustmarks are fairly simple:

- **No exchange:** The site will not capture any personally identifiable information for anything other than billing and transactions.

- **1-to-1 exchange:** The service will not disclose individual or transaction data to third parties. Individual usage and transaction data may be used for direct customer response only.

- **Third-party exchange:** Basically, buyer/disclosed beware! The service may disclose individual or transaction data to third parties, provided it explains what personally identifiable information is being gathered, what the information is used for, and with whom the information is being shared.

Of course, the devil is in the details -- or in that phrase we italicized: "provided it explains...." What exactly will it do with the data, and to whom will it be provided? Are those third parties bound by eTRUST too? Probably not.

**Raising awareness**

Everyone involved with eTRUST stresses that it is just a pilot program without final answers; it is just a worthy first step. Its goal is not to ensure universal privacy, but to get users to ask and Websites to explain. The underlying assumption is that an informed market works better, and that customers need some guarantee that the information they get is true. Informed consumers can negotiate better deals individually, and shift the market towards more customer-friendly behavior in general.

eTRUST will work not by giving people new rights, but by encouraging people to exercise their existing rights and market power and by providing a model of how the market can work best by informing its participants. The Trustmarks call users' attention to the proposition that their data may be valuable and should be protected. Then they need to read further to find out exactly what the vendor is proposing.

eTRUST is a brand name; the premium value it indicates -- its secret ingredient or unique selling proposition -- is validation of the promises behind the Trustmarks. An audit by an accounting firm is a much better way of fostering compliance than a lot of regulations. "We want GAAP [Generally Accepted Accounting Principles] for information practices," says Lori Fena, executive director of EFF.
What do they (want to) know?

Merchants' excitement about the Web includes the fact that it's so much easier to track a Web user's activities than, say, to correlate what a television viewer watches with his subsequent purchases. Web-sites can keep track of what a person looks at, how long he stays, which ads provoke the best response, whom he communicates with, what he says (in public discussion groups), how behavior changes over the course of a day. Do drinkers buy more stuff in the evening, when they've had a few? Are customers of Web catalogues more price-sensitive than customers of paper catalogues? Are people who book airline seats through the Web more likely to be no-shows? Are customers getting so sophisticated that middle seats will have to be priced lower to sell? Alternatively, would you be willing to pay extra for an aisle seat? The possibilities for one-to-one everything are endless.

In principle, a merchant could compare a person's musical tastes to his reading preferences, the political Websites he visits to the magazines he reads. It could scour the newsgroups and send e-mail to all people whose comments appeared on a particular site or matched a particular profile (as measured by statistical sampling of words). Using the new directory services, a merchant can match up e-mail, name and address...and other data linked to any of these. Try it on yourself. Thought your comments on libertarianism went only to people on that newsgroup? Think again! How did they get your name for that spam about a Caribbean island with a friendly government?

Some of this information is just statistical, but for a lot of it, marketers want need to track you individually -- Merchants would also like to know how what you see affects your subsequent behavior: Do you see something online and then go buy it in a store? Of course, the marketers don't really care who you are; they just care what you (can be induced to) buy. They want to be able to predict behavior. The problem is that the information they gather has a way of spreading further...

"Third-party attestation"

What do the accounting firms do? Here's the view of one of them, Coopers & Lybrand. C&L is not a random choice; the firm has made an aggressive strategic move into what it calls "Computer Assurance Services." Over 1500 of its 70,000 professionals worldwide work in this practice. "Clients have some anxiety about computer technology: Will it lose them control of their business," says Russ Sapienza, the New York-based partner leading C&L's Internet Assurance practice, a 150-person subset of Computer Assurance. Internet Assurance focuses on a small handful of areas, notably privacy reviews, Website audience measurement and security (firewalls and the like).

C&L's eTRUST clients include Firefly (Release 1.0, 11-96), InterMind (a privacy-oriented publishing intermediary that lets you receive tailored content anonymously), and Narrowline (page 18). "Given the relative lack of trust and confidence in Web-based commerce, these companies need a way to
demonstrate the integrity of their particular service or product offering," says Sapienza. "Independent third-party attestations from C&L over mission-critical components such as control over user data, accuracy of billing and advertising click-through rates, offer reasonable but not absolute assurance that the business practices operate as intended." In an attestation review, the client makes specific assertions, which are then "attested" to by the independent auditor. These attestation reviews are governed by American Institute of Certified Public Accountants standards of practice.

For a Web-oriented client, the firm can support any of three stages: system design (establish audit, control and security requirements), system implementation (configure system and processes), and post-implementation assessment (validate that the control system is well designed and works as intended). Sapienza notes, correctly, that all three are never-ending: Systems must be reassessed and updated, and procedures must continually be refined both to combat erosion and to adjust to new technology -- particularly in security, which is basically an arms race with malicious crackers and negligent employees.

And now a word from the other sponsor...

Roger Siboni is newly elected deputy chairman and chief operating officer of KPMG. The firm's partners elected him in part to accelerate its growth into new business areas, especially those enabled by computer technology. He divides them into two areas: new forms of attestation, which includes security and risk management as well as traditional auditing, and electronic commerce. Attestation is concerned with boundaries and what might cross them, says Siboni; electronic commerce is concerned with the implementation of what happens within the boundaries.

Whereas accounting traditionally was concerned with snapshots -- preparing books that are accurate as of a given moment -- the new world requires accounting firms to focus more on flows and processes rather than amounts and moments. eTRUST attestation is just one example of this new approach.

To do this, KPMG is radically reorienting its internal training. It is hiring more people from outside than previously, looking especially for expertise in a variety of industries. Dollar amounts may be the same across industries, but the processes and methodologies that create the dollars vary dramatically. For example, in the online business, you need to understand customer acquisition costs, churn rates, customer behavior -- to have any hope of assessing whether allocations for marketing make sense. When depreciation was spread out over 25 years, industry expertise didn't matter, but it matters a lot whether a customer is likely to last two months or two years when you want to record customer-acquisition costs properly. Likewise, privacy is a matter of procedures, not numbers.

Says Siboni, who recently moved from Palo Alto to New York City to take his new post and push the firm's efforts in high-tech consulting: "If we don't do it, others outside our profession will!"

-------------
Trust, but verify. -- Ronald Reagan
-------------

Release 1.0 19 February 1997
Site oversight

Of course, neither firm can guarantee privacy any more than it can guarantee solvency. In conjunction with eTRUST they offer a compliance mechanism -- a license subject to review. "Once the pilot is finished, we'll probably go back and tweak the process," says Sapienza. "And we'll keep reviewing things. My experience is that the security environment degrades over time. You walk away and go home, and the guard goes down again, only to be tightened up when the next review takes place." We note: It's also a good source of recurring revenue.

The presence of a third-party auditing firm adds elements of oversight and trust to the eTRUST program. Obviously, any accounting firm could do the same, but eTRUST is an education and branding campaign as well as a compliance system with licensed auditors. (For example, C&L has audited Juno's privacy practices (page 19), but Juno is not (yet) involved with eTRUST.) Over time, eTRUST will have competitors. And obviously, eTRUST itself is eager to sign up as many accounting firms as it can. Nonetheless, C&L and KPMG have a special relationship with eTRUST and more credibility because they helped design the whole program. They have both put in pro bono sweat equity in working directly with eTRUST, but they are charging their participating clients.

Speaking of $$$$ 

While it should cost very little to participate in eTRUST itself, it does cost a lot to be properly certified, just as it costs a lot to be audited, especially for a public company. That's one of the realities of doing business. We can just hope that there will be vigorous competition in privacy attestation services as in other markets, and that supply will rise quickly to meet demand.

Although Webmasters who post the eTRUST logos on their sites will eventually have to pay a "small, graduated" fee to eTRUST, the service right now is free. (The terminology is awkward, but here's a try: "Users" are end-users, customers, people who visit a site and who read and rely on the logos. "Logo-posters" are users of the logo, but we call them posters to distinguish them from their customers. A third class of users are the firms licensed by eTRUST who validate the logo-posters' claims, usually accounting firms; we call them "third-party attestors.")

As noted, logo-posters have to pay their third-party attestors commercial rates for the validation service; that's between the attesting accountants and their logo-posting clients. The accounting firms will also have to pay eTRUST a license fee. Beyond that, eTRUST is still working out its precise business model; it cannot support itself during its first couple of years. To the extent possible, we believe eTRUST should get its funds from the accounting firms -- the people who get tangible revenue due to the program -- rather than from the logo-posters. After all, the accounting firms have an immediate vested interest in the success of the project, although in the long run the logo-posters will find it useful in attracting customers...or so the plan goes.
Pilot preliminaries

Money flow is only one of the issues the pilot is intended to sort out. Exactly how much work does it take to test for compliance? How often should logo-posters' claims be spot-checked? What are the vulnerabilities? Are the logos and their explanations intelligible to users?

What happens when someone fails in compliance? That's part of what eTRUST hopes to determine during the pilot and over the next year -- ideally without too many instances of non-compliance, but enough to show that the program is for real. The initial steps are cancellation of the right to use the logo and posting the wrong-doer on a "bad-actors" list; of course, the wrongdoer has to pay the costs of determining its non-compliance and ultimately could be sued for fraud. But stiffer, quicker penalties may be needed: The conditions shouldn't be so onerous that no one signs up, but they should be severe enough to be meaningful. Breaches are likely to be noticed through spot-checks by the third party attestors. Other sources of challenges are whistle-blowing employees or aggrieved users, although it's usually difficult to figure out who compromised your privacy.

The data processing requirements behind privacy protection are also challenging, since some data will need to be tagged to be used only in certain ways. All we can say is, privacy protection is a great employment opportunity over the long run.

There will also need to be contracts specifying the sanctity of the data as companies form, merge and break up. Do the contracts governing the use of data survive a bankruptcy proceeding? They should.

We're putting more and more power in the hands of users. How do you educate them to make an informed decision, when all they ask for is simplicity? But if we don't do this, we'll all become like children under the law, with no ability for informed consent.

-- Lori Fena, executive director, EFF

THE INTERNET PRIVACY WORKING GROUP

Independently responding to many of the same pressures as eTRUST, the Internet Privacy Working Group was convened by the Center for Democracy and Technology in Washington. Its planned "product" is a technical standard called P3, for Platform for Privacy Preferences. The IPWG is in many ways a continuation of the group that produced the PICS content-labeling standard, and includes many of the same players. Members include America Online, Microsoft, Consumers Union, MCI, Dun & Bradstreet, IBM, AT&T, the Direct Marketing Association, the Electronic Frontier Foundation, eTRUST, the Coalition for Advertising-Supported Information and Entertainment, the National Consumers League, the Interactive Services Association and at least indirectly the members of the World Wide Web Consortium (W3C), which developed PICS and is developing P3. (PICS stands for Platform for Internet Content Selection and is a standard protocol for labeling Internet content; we described it at length in Release 1.0, 12-96.)
Speakable privacy

Since the P3 vocabulary is not yet developed (it's due this May), the following is merely a thought experiment, to give some idea of how P3 might work in practice.

P3 will be designed to let people define privacy preferences for themselves and embed those preferences in a browser or software agent that can communicate directly with Websites and other electronic partners. The user agent could select vendors that meet the user's privacy preferences, or perhaps even negotiate suitable conditions. The task of defining privacy preferences in a way that allows such automatic execution and negotiation will be much like the process of drawing up an insurance policy or a will -- confusing to the uninitiated. P3's existence should loose hundreds of creative people on the job of building tools to help people express their preferences, probably with branching questionnaires, heuristics and other clever approaches. There might be defaults for children and perhaps for medical information. Low-end tools may offer three canned options with little flexibility.

Says Jerry Berman, chairman of CDT, "You can't just allow people to express their preferences and then they're done. They'll end up missing the sites they might want to see." So a clever tool would say, "Do you really not want to reveal your income to anyone? You may miss out on interesting information about exclusive vacation spots, jewelry, yacht charters. If you are interested in meeting people, you may miss some interesting people with shared interests.

"Alternatively, if your income is low, you may miss interesting offers for budget cruises, exciting ways to earn money in your spare time, student loans and other valuable offers..."

As with wills, people will be able to use automated tools to express a relatively simple set of preferences; those with complex lives may want to sit down with a privacy expert (probably from an accounting firm, of course) to develop a complex set of preferences.

For example...

I don't want to reveal my age...unless I get a senior citizen's discount worth more than 10 percent of the price of an item or $400 in absolute value. (That info cannot then be reused; I don't want to get any catalogues for walking aids, retirement homes or annuities.)

I don't want to reveal my income...unless it's required to see sites offering jewelry and vacations at exclusive places in the Caribbean.

I'd like British Airways and Lufthansa to know how much I fly with American and Delta. Maybe they'd treat me better!

I'd like to be visible to other single women between 35 and 45 in my discussion groups, but not to any men at all. [That may be a stretch for now.]
The IPWG plans to produce substantial technical work later this year, but the first step is to come up with a vocabulary. "We want to develop a vocabulary so people can accurately and explicitly describe what they want, so they can craft their preferences," says CDT's staff counsel Deirdre Mulligan, who is shepherding the project. The group hopes to develop demos for user testing by May, and then the developers at W3C can take it from there for implementation.

P3 in practice

While content rating requires some formatting, its vocabulary is fairly free-form; any third-party rating service can establish its own terms and definitions. By contrast, a privacy vocabulary is more complex, and needs a grammar for expressing conditional preferences. That will enable not just static labeling of privacy practices, but actual negotiation between a customer's self-described preferences and the options a site offers. (See box across.)

Using P3, a user could specify what kind of privacy rules he wants to find or avoid, and his browser or other tool could implement those preferences automatically. A P3 program at the Website could describe its own practices and also read a user's self-description. The two agents would then negotiate the terms of a transaction. At its simplest, this might mean that the user could see/use only certain pages of a site that meet his privacy criteria. Special areas would be reserved for those willing to part with certain information. But as use of P3 spreads, users and sites could automatically negotiate far more complex interactions.

Would users trust such an automated system? That would depend in part on the auditing/compliance system behind the scheme. (The user's and the site's choice of auditor or auditing scheme could of course be specified in the label.) For all the same reasons as for eTRUST, IPWG label-posters will also have to devise some provisions for attestation -- or ally with eTRUST -- if P3 is to have any credibility. With such a validation/enforcement structure in place, P3 could have immense power.

---

4 Note that eTRUST Trustmarks are a logo for people to see on a Website; P3 labels are executable code for a browser or other software tool to read and communicate with.

Release 1.0	 19 February 1997
MAKING IT REAL

How can these two complementary systems succeed? This question is of broad interest, since these two groups face the fundamental challenges of anyone trying to foster self-regulation in order to forestall government regulation. The Boston Consulting Group volunteered to do a pro-bono assessment of eTRUST's positioning and prospects, and its mid-term findings promise some interesting conclusions, for eTRUST specifically, for P3 and for other such efforts in the future.

The main conclusion is simple: eTRUST, P3 and efforts like them rarely work without a "hammer." As BCG's Andy Blackburn delicately puts it, "Adoption is a long walk through the mud unless you have some externally applied sense of urgency." That's not necessarily just the government, he notes, but the threat of government action may well promote urgency in other sectors...

Hammers over our heads

Currently, the government is indeed paying substantial attention to privacy issues on several fronts.

The Federal Trade Commission is conducting a long-term Privacy Initiative and is planning a privacy workshop to study technical tools and self-regulatory models to protect privacy -- an effort in the right direction. (In our December issue we quoted Federal Trade Commissioner Christine Varney as basically in favor of "voluntary systems of standards or ratings, whether for privacy or content...backed up with strong government enforcement against misstatement as either deception or fraud." We hope that's a fair statement of your attitude, Christine!)

At the same time, the Commerce Department's National Telecommunications and Information Administration is compiling a report on the issues around privacy self-regulation. "As a general matter," says NTIA chief counsel Barbara Wellbery, "we favor self-regulation, but self-regulation with teeth. But people say self-regulation, and that's the end of the conversation. We're looking at self-regulation more analytically: to see where it works, where it may not work -- for example, medical information and children come to mind... If you do it, what do you do about antitrust? How do you handle enforcement? What role can technology play in all of this?" eTRUST and P3 should provide useful fodder for all these questions -- while Commerce's interest may be a hammer encouraging industry to do something for itself.

Both these efforts look promising for self-regulatory efforts such as eTRUST and P3. However, there are also several bills pending in Congress: the Consumer Internet Privacy Protection Act of 1997 (Rep. Bruce Vento, D-MN); the Children's Privacy Protection and Parental Empowerment Act (Rep. Bob Franks, R-NJ) and the Communications Privacy and Consumer Empowerment Act (Rep. Ed Markey, D-MA). Whatever they are now, there is no telling what these bills may become as a result of political negotiations in Congress, where the focus is more on government regulation than on market-based solutions. Nor would the laws apply overseas, as both eTRUST and P3 will.

So can eTRUST and P3 beat Congress to the punch? And ironically, will the government's activities hasten adoption of eTRUST and P3 in the marketplace?

Release 1.0 19 February 1997
Controlling the sorcerer's apprentice

What BCG found out is not surprising. Industry disclosure schemes often founder without strong government/public pressure. Otherwise, companies are simply too busy to adopt them, and customers don't factor the information disclosed into their buying habits. eTRUST's and IPWG's challenge is to raise the public's awareness just enough to make it want eTRUST and P3, but not enough that it puts the issue into the hands of government.

Perhaps the most successful disclosure rules are those of the National Association of Securities Dealers; not surprisingly, they are mandated by law. Other schemes allow opt-in and opt-out, such as movie or television ratings -- but the entertainment industry as a whole adopted them in direct response to the threat of worse from the government. (From our perspective, the systems are not entirely satisfactory, since they involve central rating systems rather than a diversity of opinion and enforcement.) In many cases, BCG found, there is some complementary sector that forces self-regulation: In the case of movies, it was the theatre owners; in the case of Underwriters Lab, it was first insurance companies and then retailers. For BPA International (formerly the Business Publishers Association), which audits business publications, advertising agencies forced regular auditing of circulation and other claims.

Beyond the hammers: Making the case

So beyond government "hammers," what are the forces that can encourage P3 and eTRUST? Who can play the role of hammer for eTRUST and IPWG, or for privacy self-regulation generally? "Anyone who provides a conduit between merchant and customer could potentially exert such influence," says BCG's Blackburn. "Browser vendors and online services could offer privacy filters" much as many now offer (mostly optional) content filters.

Other possible players include the credit card vendors or newer payment and verification systems, on the one hand, and accounting firms on the other. The payment/verification systems need a lively new market which they could serve, and the accounting firms are looking for new forms of business -- specifically, attestation about privacy and security practices. Is this enough to force the issue?

However, credit card companies are not so enthusiastic. They and their partner banks have significant interests in the use and exchange of customer information. Says Blackburn: "Big brand names, including credit card companies, say, 'We are a trust logo. But if some major players got involved, we'd go along.'" To some extent, we believe, most major vendors and financial companies would not mind strong privacy-protection practices as long as their competitors were hampered by the same restrictions. It's simply that no one wants to go first.

Among the merchants -- potential logo-posters -- themselves, what kind of firms are most enthusiastic about eTRUST? Primarily smaller, less-known firms who ask customers personal questions about finances, health and the like. Unfortunately, those middle-market firms don't have large budgets to spend on auditing. Nor are they influential in persuading other firms to follow suit.

Release 1.0 19 February 1997
Larger firms with existing customer bases and reputations don't need eTRUST and P3 so much; the truly bad actors don't want them. For the larger firms it's not merely a question of brand recognition and size, Blackburn clarifies. Big firms with good reputations are also likely to have a lot of data from other sources, and they may not want to apply different standards for Web-source data. Nor do they necessarily want to adopt the same standards they use for Website data for all their data. They may also not want to go through the expense and hassle of a privacy audit without a clear idea of how it might benefit their business.

Nonetheless -- or accordingly -- BCG and eTRUST would dearly like to see a couple of large influential merchants adopt eTRUST. Yes, Amazon may be more influential on the Net than, say, Borders; on the other hand, traditional merchants may be much more influential among customers new to the Net.

The trick is to persuade merchants of all sizes that privacy is a compelling and vital marketing issue. There are two groups that can deliver this message most effectively: the accounting firms who see privacy attestation as a business opportunity; and customers themselves...assuming that the message is true.

Remember the customer

Yes, says Blackburn, you can't do much without a clear customer benefit. So BCG is trying to discover just what concerns consumers about privacy -- which is often confused with security. Consumers say they would be a lot more active on the Net if there were privacy, but what does that mean? Are they afraid of having a credit card number stolen? Do they simply want to know what happens to their data, or do they actually want to stop its spread? In fact, their answers vary a lot -- by vendor, by kind of data and subjectively. How much do they want that loan? Are they in a good mood?

How do we get people who don't necessarily care about privacy to do so? How can we take the generalized resistance to the Net, sharpen it into privacy concerns, and then assuage those concerns with eTRUST?

Indeed, should we? Or are we simply creating a spurious need to fill? Yes, we should. Everything tells us that customers feel more and more bewildered by the array of choices facing them. They may not worry about a telemarketer's calls, but they do feel uncomfortable at the prospect of giving personal information to strangers. eTRUST and P3 are all about giving people control to use the powers created by technology.

Where to from here?

We like eTRUST and P3 because they are not moralistic, evangelistic or dependent on government (other than for enforcement on the basis of fraud). They are simply two examples of the kind of grass-roots effort at self-regulation in all spheres that we hope to see proliferate on the Net.
CASE STUDIES

In practice, privacy protection is more than technology. How can we achieve it without making the world into a sterile place where everyone is anonymous? Customers actually like to be treated as known individuals by marketers that they in turn know and trust. After all, the rhetoric promises a global village, not a global city.

The following case studies show how individual companies can handle privacy issues, and present their practices as a customer benefit rather than a legal issue. Their practices are still evolving, along with customer preferences and pressures from those outside hammers.

Fourll: Privacy Issues in practice

Simply managing transaction data is simple compared to the privacy issues of running a directory service. For example, take Fourll, a leading Web "white pages" company. The basic service is collecting and maintaining a database of individuals' names, e-mail addresses, phone numbers and other data. The telephone data is licensed from Metromail; the e-mail addresses come from user registrations (20 percent and growing), public-domain directories on the Net (50 percent), and Usenet (declining).

People are encouraged to register; you can also ask to be stricken (even if you show up again from another source). All this data is available to anyone who visits Fourll's Website -- but only a bit at a time. Aside from its acceptable-use policies (restricting wholesale reuse and general abuse), the company has no hard and fast rules in order to be flexible enough to stop new problems as they arise. For example, the company makes it difficult for users to collect names for mass e-mailing or for building any kind of secondary database. It supplies information only one e-mail address at a time, and it monitors user activity for unusual behavior, such as downloading one address after another. (It doesn't care who you are, but it does care what you do.) Currently, when Fourll's server detects such a pattern it notifies a system administrator; in the future, it may invoke an automated response.

Also, you can't find a name from a phone number or from an e-mail address; you need to know a person's name before you can get anywhere. However, that wasn't always true. The company licensed its database to Yahoo! last summer. Yahoo! did allow reverse searching, using the Fourll data -- creating the Net's most visible, most-used reverse look-up for phone numbers. Yahoo! put it up in April last year, and it quickly became one of the most-used functions within Yahoo!’s people search. Fourll ceo Mike Santullo says he felt uncomfortable about the reverse look-up service, but both parties note that it was tremendously popular and did not actually lead to many problems.

Both companies were punctilious about delisting people who asked for their names to be removed. Meanwhile, police departments, suicide prevention centers and other "good guys" made good use of the service. "Bad guys" didn't seem to be more prevalent than the annoying people who use caller ID. But in December, in response to perceived pressure (apparently including the expectation of this article, to our surprise), the companies dropped the service. Similar information is still available, but sometimes from companies who may be less careful than Yahoo and Fourll.
It's a pity that such a potentially valuable service should be abandoned and relegated to non-mainstream providers. The moral of this story -- which is not yet over -- is that a little self-regulation or more fine-grained control over personal data may actually yield a situation where information is more readily available. But for now, it's all or nothing.

That's the long-term question: How can you make information available selectively? Fourll is addressing that in part, although not with reverse look-up for now. People willing to register with the service can get selected additional information about others; presumably, being registered themselves makes them less likely to abuse the information. For example, they are allowed to search the database for people by affiliation, such as Princeton High School, violinist, etc. This information comes from individuals and from the groups themselves; they in turn can specify what information they give should be made available, and to whom. For example, a person's initial record won't show the schools he attended, but if you happen to know (or guess) Princeton High School, that will show up once you ask specifically. Some groups let only group members query on group-oriented data, so only PHS alumni could find out that other people are PHS alumni, or what year they attended. In fact, Fourll's business model includes support of such interest groups, even as it is also addressing the mass market through alliances with companies such as Yahoo!, InfoSeek, Nynex and US West.

Yes, it sounds cumbersome and awkward and somewhat arbitrary, but isn't that the way it is in real life? The folks at Fourll have thought about all this a lot, and will refine their approach as they encounter new problems and solutions over time, says CEO Mike Santullo. The main thing is to be aware of the issue.

**Narrowline: Mediating between advertisers and audience**

Narrowline is an ideal customer for a new-style auditing firm: It sells things you can't see, and a part of the value of the service is that you can't see them -- in the sense of protecting the privacy of customers. The company is about to roll out its service, Brought To You By, a trading floor for sponsorship of content and events. Brought To You By has the granularity of a classified-ad market where what Narrowline calls "Netcasters" (content/community providers) and sponsors (advertisers) can find one another, based on the audiences they're seeking or can deliver.

Narrowline adds value to its market with metering and verification for the advertisers and privacy protection for the Netcasters and their audiences. Not only do the audiences presumably appreciate their privacy, but the Netcasters can also keep the sponsors from bypassing them to talk to individuals directly -- unless an individual makes the first approach back to the sponsor.

Founder Tara Lemmey (who spoke at last year's PC Forum; Release 1.0, 3-96) understands that a primary feature of the Internet is its support for reaching market segments, instead of broadcasting the same message to everyone -- even if you don't know each one individually. But you can't do that unless you can find and define those markets and figure out how to reach them in almost real-time. Narrowline sells access to particular demographics through sites, but doesn't pass on to the sponsors any detailed information...
about the visitors/members of the site. Obviously, the value of the service depends on rigorous integrity, both in guaranteeing users their privacy and sponsors that they are getting the demographics they are paying for even if they can’t see them. In that context, Narrowline is an ideal customer for C&L, because it needs auditing for just about everything.

When the customer visits a site sponsored by a Narrowline advertiser, the text and editorial come from the Netcaster, while the banners come from Narrowline and its advertisers. Narrowline meters the banners and knows who’s receiving them. It provides a barrier with assurances to both sides: That their identity is safe to the customers, and that the demographics are reliable to the advertisers.

What this means is that the customer simply has to trust Narrowline instead of all the advertisers he may encounter. For now, however, consumers don’t necessarily know Narrowline either, but its use of the eTRUST Trustmarks means that the eTRUST brand will be applied to advertising from sponsors who don’t sign up with eTRUST specifically. The sponsors get demographics they can trust, but they don’t have to go through the trouble of an eTRUST audit because they never see the data that only Narrowline collects.

Narrowline's approach raises an issue that will increase in visibility as more and more Websites are acquired by other companies or join alliances. Just how broad is the entity to whom you are giving your information? Can you trust it? Or is it really "they"?

Juno: Free e-mail in exchange for your information

Many sites and services make more explicit bargains. Juno, for example, offers customers free e-mail in exchange for exposing the user to specific advertising based on the user's characteristics. The service has been a success with end-users: About 1.5 million people have signed up for it, filling in a detailed profile in exchange for free e-mail. They do not have to have Internet access, since Juno offers its own local dial-up throughout the US, and they do not get Internet access, but they can send and receive e-mail across the Internet. They can also view graphics-filled ads from Juno's advertisers and from Juno itself. The site looks something like a Website, and its ads look like Web banner ads, but the only people who can use it are registered Juno customers.

Although the service is free, it's not quite "the people's e-mail." It still skews Internet-wards, says Juno president Charles Ardai: mostly male and higher income. You may not need to pay for Internet access, but you still do need a computer with a modem.

The users' identity is not revealed to the advertisers, who simply get a report such as "5482 men between 18 to 49 who have expressed interest in a new car saw your ad last month; please pay $2,741 within 30 days." Juno may also tell them, for example, that 25 percent of the people who clicked on their ad were female.

But how is an advertiser to know this is true? Juno's financials and other numbers, including claims to advertisers, are audited by Coopers & Lybrand. "Unlike a Website, we're pretty simple to audit," notes Ardai. The only
people who visit are its own registered and profiled customers, using Juno's own software.

On the revenue side, Ardai isn't ready to proclaim victory, but he notes a set of repeat advertisers: American Express, Lincoln Mercury, Miramax, Okidata, Bausch & Lomb. "When we hit a million members, major advertisers started returning our calls," he says.

Juno has discovered that it can also sell products itself to its customers -- a cookbook to someone who's indicated an interest in cooking, for example. She can send back a purchase order with ease, he notes, and her credit card never goes over the Internet. (That may not be a real issue, but it makes some customers feel more secure.) And people who respond to an advertiser's direct offer, of course, lose their anonymity.

Given that this is a free service, we wondered if there were any people who might be left out, if their demographics just don't meet any advertisers' criteria. That could happen as far as advertisers are concerned, says Ardai, but it sends its at least some of its own product offers to each of its customers. And it allows anyone to be a customer. As a private company, for now, Juno can afford to serve everyone -- founder David Shaw's quiet little contribution to the public welfare.

---

Release 1.0 is published monthly, except for a combined July/August issue, by EDventure Holdings, 104 Fifth Ave., New York, NY 10011-6901; (212) 924-8800; fax, (212) 924-0240. It covers PCs, software, the Internet, computer-telephone integration, online services, groupware, connectivity, messaging, wireless communications, Internet-oriented law and other unpredictable topics. Editor: Esther Dyson (edyson@edventure.com); publisher: Daphne Kis (daphne@edventure.com); managing editor: Jerry Michalski (spiff@edventure.com); circulation & fulfillment manager: Robyn Sturm (robyn@edventure.com); executive assistant: Helen Martin (helen@edventure.com); assistant circulation & fulfillment manager: Scott Giering; administrative assistant: Susanna Stromberg (susanna@edventure.com); editorial & marketing communications consultant: William M. Kutik (kutik@edventure.com). Copyright 1997, EDventure Holdings Inc. All rights reserved. No material in this publication may be reproduced without written permission; however, we gladly arrange for reprints or bulk purchases. Subscriptions cost $595 per year, $650 overseas.

Release 1.0 19 February 1997
EPILOGUE: BEYOND WEBSITES, BEYOND LABELS

Issues: What's the difference between buying from L.L. Bean online and through mail-order? What's after eTRUST? Can online practices affect the real world? Once we feel safe will it matter less?

The issues of privacy didn't begin with the Internet, and they can't be resolved by controlling what happens on any, or even all, Websites. The problem occurs among Websites -- and away from them -- in the places where people and companies assemble databases of information gleaned from many Websites and from non-Web mailing lists, directories, news reports, listings ...and other databases. A lot of this information has traditionally been available to people willing to go to a lot of trouble, visit county document vaults, call companies posing as a prospective employer or old boyfriend, or spend a few hundred dollars to get an investigator's license. It has also been available on a random basis to criminals in jail doing data-entry work, bored clerks in the IRS and various other untrustworthy people in trusted positions.

Many companies, notably Equifax, Metromail, some credit-card providers and many others manage huge amounts of such data and trade it among themselves. Yes, it makes the economy more efficient and keeps revenues up and costs down. But not all of the companies who manage this information are not especially trustworthy -- nor are all their employees.

The presence of the Web increases the ease of assembling such data for a broader range of people. It is precisely the interconnectedness of the information that makes safeguarding privacy such a challenge. Indeed, what people are concerned about is the combination of data from different sources: Web behavior, buying habits, travel history, income data... Often, facts are innocuous until they're combined with other facts.

The user wants a seamless experience as he explores the Web, but he wants to appear as a discrete entity to each place he visits. The challenge is for a person to have a legitimate identity revealed as appropriate, with a credit rating, an employment record, a bank account and a medical history.

Right now, a person's identity usually gets splashed all over the Net in little fragments -- no problem. The user wants to keep the fragments fragmented. But then someone in particular -- anyone from a benign marketer only after the customer's business, to an employer, a stalker or a blackmailer -- can start collecting those fragments. One version of the problem is when the data are incorrect; another version is when they are true.

In the end, we can set up systems to foster privacy. We can require employers to check the credentials of employees, spot-check work practices and take due care. We can't totally guarantee everyone's privacy, but we can create a situation where people get to choose what level of privacy they want -- or can get -- and a means of recourse when promises are breached.

Moreover, the Net will create new privacy-related issues. Consider the coming controversy over linking. You may freely publish certain information, putting it into the public domain for public use (if not commercial resale). But what control do you have over a parody that links to your site? None -- but a lot of people feel injured by such links -- especially uptight.

Release 1.0

19 February 1997
corporations paranoid about control... sorry, especially stakeholder-ori... especially stakeholder-oriented corporations concerned with maintaining their public image as part of their fiduciary responsibility.

So... We can't help thinking that in the distant future our era will look like the dim past -- a time when people walked around like shadows, insubstantial figments with little information about them visible. The late 20th-century notion of privacy will seem like an aberration. What is it people are so scared of? It's not really clear. But it is clear that we won't go forward into the future unless we feel we're in control.

Beyond labels: Agents

By now, it should be obvious that labels can operate in many spheres. With application code, they can even perform negotiations. In fact, labels are nouns that rule-based agents can use...

A browser could specify how much a person was willing to pay, and the person would not see any pages that cost more than 10 cents per page, or that did not honor a certain brand of electronic cash. A blind person could search only for sites that include text descriptions of their graphics. Anyone could select by language, political slant or religious affiliation. A New Yorker could wish to see only sites rated reliable by The New York Times. An accused felon facing conviction could search for lawyers certified to practice under a certain jurisdiction; an investor could look for banks with interest rates below 8 percent (and Moody's ratings above BBB).

You could also use standard labels for collaborative filtering (see Release 1.0, 11-96). Currently, the collaborative filtering tools/services do this with their own proprietary formats. However, Firefly, a member of eTRUST and of the PICS consortium, has just released a public-domain API for its collaborative filtering system -- a first step in this direction.

Ultimately, PICS, P3 and other labeling systems will turn into machine-readable protocols for specifying almost anything. They may end up being so extensible that they almost vanish as standards into thousands of specializations, but that's a good way to start. If you look at the history of agents, the problem is that except for generic tasks such as filtering content, it's hard for agents to do much outside of a hermetically sealed "trusted" environment: A specific agent knows how to order from a specific catalogue. EDI is one example of such a highly specified language.

So if today's standards disappear into a haze of specific implementations, they will have served their purpose: People and places can describe themselves and their own rules of engagement, and others can interact with them safely on the basis of those descriptions. The only requirement is that those self-descriptions be accurate. That may end up being a big job for third-party certifiers and raters. And of course third parties can also provide ratings without the consent of the rated -- but with precisely the amount of credibility they have earned in the marketplace.
RESOURCES & PHONE NUMBERS

Michael Kleeman, Andy Blackburn, Theanne Thomson, Boston Consulting Group, (415) 732-8060; fax, (415) 732-8200
Deirdre Mulligan, Jerry Berman, Center for Democracy and Technology, (202) 637-9800; fax, (202) 637-0968; berman@cdt.org; www.cdt.org
Russ Sapienza, Coopers & Lybrand (New York), (212) 259-1517; rsapienza@colybrand.com
Barbara Wellbery, Larry Irving, Department of Commerce, National Telecommunications and Information Administration, (202) 482-1840; (202) 482-1635; lirving@ntia.doc.gov
Pat Faley, Direct Marketing Association, (202) 955-5030; fax, (202) 955-0085; pfaley@the-dma.org
Lori Fena, Stanton McCandlish, Electronic Frontier Foundation, (415) 436-9333; fax, (415) 436-9993; lori@eff.org, mech@eff.org; www.eff.org
Andrew Boer, eTRUST/CommerceNet, (415) 858-1930 x207, fax: (415) 858-1936, aboer@commerce.net; www.etrust.org
Christine Varney, Federal Trade Commission, (202) 326-2171; fax, (202) 326-3441; cvarney@ftc.gov
Ted Kamionek, Saul Klein, Firefly Network, (617) 528-1000; Saul_Klein@firefly.net
Mike Santullo, Fourll, (415) 617-2012; mike@fourll.com
Charles Ardai, Juno, (212) 597-9226; charles@juno.com
Roger Siboni, KPMG Peat Marwick, (212) 909-5005
Tara Lemmey, Eric Theise, Narrowline, (415) 975-5300; fax, (415) 975-3808; verve@narrowline.com, tara@narrowline.com; www.narrowline.com
Ron Plesser, Piper & Marbury, (202) 861-3969; fax, (202) 223-2085; replesser@pipermar.com
Charles Jennings, Portland Software, (503) 220-2300; cj@portsoft.com
Tim Dick, WorldPages, (415) 536-0680; tim@worldpages.com
Jim Miller, Joseph M. Reagle Jr., World Wide Web Consortium, (617) 258-7621 and 253-3194; jmiller@w3.org, reagle@mit.edu, reagle@w3.org; www.w3.org/pub/WWW/PICS
Jerry Yang, Tim Koogle, Yahoo!, (408) 731-3300; fax, (408) 731-3510; jyang@yahoo.com

Except as noted otherwise, all companies’ Websites are at the likely address, http://www.domain_name.com.

---------------

COMING SOON

- Relationship and link management.
- Navigation.
- Market-based security.
- The analog world.
- And much more... (If you know of any good examples of the categories listed above, please let us know.)

Release 1.0

19 February 1997
Please enter my subscription to Release 1.0 at the rate of $595 per year in the U.S. and Canada. Overseas subscriptions are $650, airmail postage included. Payment must be enclosed. Satisfaction guaranteed or your money back.

Name__________________________
Title__________________________
Company_______________________
Address________________________
City___________________________ State_________ Zip_________
Country________________________

Telephone________________________ Fax________________
E-mail__________________________ URL________________

☐ Check enclosed.
☐ Charge my
  ☐ American Express  ☐ Mastercard  ☐ Visa
Card Number_________________________ Expiration Date_________
Name on Card________________________ Signature________________

☐ Please send me information on your multiple-copy rate.

Please fill in the information above and send to:

EDVENTURE HOLDINGS INC.
104 FIFTH AVENUE, 20TH FLOOR
NEW YORK, NY 10011

If you have any questions, please contact us at 1 (212) 924-8800;
fax 1 (212) 924-0240; e-mail us@edventure.com; www.edventure.com.

Daphne Kis
Publisher