PRIVACY PROTECTION: TIME TO THINK AND ACT LOCALLY AND GLOBALLY
by Esther Dyson

In this newsletter, we normally tell you about things; we don’t tell you to do things. But this month’s issue is a little different. The situation with regard to personal privacy protection is reaching a turning point in the United States. We are posting this issue of the newsletter on our Website at www.edventure.com/privacyaction to encourage wide dissemination of its message; we welcome links to the page or reasoned comments to edyson@edventure.com. (Let us know whether they are for publication.) Finally, see page 3 for a personal message that matches your own situation.

Over the next few months, businesses, other organizations and consumers in the US will have the chance to prove that we are capable of handling at least some of the issues surrounding individuals’ control of personal data—or not.

If we do not do so, the US government will work up a set of laws designed to guarantee so-called “personal privacy.” These laws are likely to be complex, inflexible, difficult to implement, and worst of all counterproductive when applied to the Internet, which operates outside the US as well as within it. Among other things, the US will need to coordinate its policy with other countries, most notably those of Europe, which are also lurching towards some common policy.

It’s not that any government involvement at all is bad. Without government prodding and disclosure requirements, the transparent market for privacy might not emerge at all. Moreover, traditional governments themselves are part of the self-organizing market for governance systems we hope will emerge.

(We define a market as a place where people can make choices. In the long run, we hope people on the Net will be able to choose under which government’s or other jurisdiction’s rules to operate in each sphere of online activity.)

WELCOME, KEVIN! SEE PAGE 33
Meanwhile, governments maintain the necessary courts, recourse systems and the like that are still lacking in cyberspace. Banishment, the primary punishment possible in cyberspace so far, is hardly sufficient to deter serious malefactors. Thus, we foresee a market of coordinating, collaborating and competing jurisdictions rather than one in which traditional governments are absent. We also envision a market where leading businesses vie to educate the public because they believe an educated marketplace gives them an advantage.

What’s at stake

The future of the Internet and its governance mechanisms hangs in the balance. Privacy is an important issue, and one that resonates fiercely in the hearts of the public. It definitely deserves attention and resolution. But the way we handle privacy will also serve as a model for governance on the Internet overall: Services such as TRUSTe offer a new way of establishing jurisdiction, guaranteeing people’s rights and offering them choices in cyberspace. Organizations such as the Council of Better Business Bureaus and the Direct Marketing Association, though less focused on privacy, also offer dispute-resolution mechanisms that could serve in this way. The industry’s efforts to educate citizens about their rights (if only to win their business) offer an example of how enlightened self-interest can foster the public interest. All this will happen not through a central authority, but rather through the interactions of many authorities who consider themselves or would like to be central...but are not.

Thus, this is not a mere “Internet industry” issue, but rather a challenge for the world going forward. When people talk about “global” this and that, this overlapping of jurisdictions underlies everything they mean. If these issues of governance don’t get resolved, it is a problem for the world, not just for the Internet. (Shades of Y2K.)

In this issue...

Little of the information that follows is new to inside players, but it is more than the official story. Our aim is to get it out into the real world, where people and organizations can act appropriately to make the right things happen. Please play your part!

Disclosure: Esther Dyson has some involvement with two of the organizations discussed here. As chairman of the Electronic Frontier Foundation, she was indirectly involved in the creation and sponsorship of TRUSTe. Now, as a board member of the EFF, she continues to serve as an informal advisor to TRUSTe. Second, she was a small shareholder (under 0.1 percent) in Firefly, through an initial investment in NetAngels, which was sold to Firefly.
WHAT YOU CAN DO

If you’re Bill Gates, information industrialist: By appealing to consumers and the public interest, you can help keep Joel Klein off your back. Use Firefly’s expertise in the public-domain P3P “privacy” technology to work in collaboration with the World Wide Web Consortium. Build user-friendly tools on top of it for competitive advantage: data-management controls for users, along with server-side data tools. Promote consumer empowerment as central to the new Digital Nervous System you’re promoting (interacting neurons, if you like). Remember what Ford did with the $5-dollar day: Other industrialists thought he was nuts, but he was creating a market for his products that went way beyond his own employees. He raised the bar and doubled wages nationwide. To their amazement, businesses benefited: One company’s employees were another’s customers. Likewise, your empowered users will lose their fear and be active customers for every vendor.

If you’re Joel Klein: Use the leverage you have to get Bill to do the right thing. Encourage Microsoft to keep working with the World Wide Web Consortium to keep the underlying technology standards improving and freely available. Quietly encourage Netscape to call Microsoft’s bluff and offer its own version. Build a bridge to Europe.

If you’re Jim Barksdale: Take the initiative. Keep working with Firefly/Microsoft and W3C on user-privacy technology. Then, get all those third-party source-code hackers to help you incorporate it into the next release of the browser with your own tools and interface, or do it yourself. Make good on your idea of building in a feature that looks for a privacy statement and notifies the user if it’s absent.

If you’re Lou Gerstner: Take advantage of your own power. After all, it was you standing next to Bill Clinton last July at the Framework for Global Electronic Commerce festival (sorry, we mean “announcement”). You can set the agenda both with your own corporate clients and with the public. If you support the Council of Better Business Bureaus, make sure its programs is industrial-strength. Come up with a killer ad campaign and take the high ground. Big business is your market, and you’re much more persuasive with them than all those Internet types.

If you’re Steve Case: You’ve been talking the talk, and even trying to walk the walk. (AOL’s recent glitches have been embarrassing, but your heart and your policies are in the right place.) Like it or not, you’re a spokesman for the Net. Don’t be shy; use privacy as a marketing message.

If you’re the World Wide Web Consortium: Hire a good PR guy. Become open and friendly. You operate in the public interest; you control technology (P3P) that individuals could use to protect their privacy, but your organization is hard to reach and your Website is confusing. Remember that openness is not just technical or legal; it’s attitude!

If you’re TRUSTe: Round up some more support, and try to find a bad guy to go after to gain some credibility. Convince businesses that voluntary liability and choice of venue is preferable to mandatory liability and a patchwork of jurisdictions. Start delivering on your promises, and disclose your own practices better. Make up your minds whether you stand for disclosure, or for some particular standards of privacy.
If you’re the US Administration or Congress: You’ve sent about as many messages as you can. Finally, the folks are beginning to listen. Sorry it took so long! Be patient for a couple more months without relaxing the public pressure. It will pay off, and then you can devote your scarce energies to more useful tasks, such as fixing the IRS, Y2K, Social security and pleading the case for the decentralized approach (don’t call it “the US approach”) to other governments. If you must “do something,” focus on disclosure and rules concerning kids and medical information. You could also do something about tightening the rules for protection of personal data collected by the government - or reduce the amount collected overall.

If you’re an accounting, insurance or law firm: This is a great opportunity for recurring revenues. Build a data-protection assurance practice, fast. Tell your clients they’re at risk, and help them figure out how to reduce the risk. Support the AICPA’s WebTrust program, and get the AICPA to put some teeth into it.

If you’re an advertiser or merchant: Remember you need customers’ trust; you have to earn it. Your customers do want to tell you all (or almost all), but remember your loyalty should be to them and not to other merchants. Don’t sell (out) your customers’ trust to make small change on the side through list rentals or dubious cross-promotions. And don’t be shy about promoting your data-protection practices. (If you rent lists for a living, find another business!)

If you provide programming services, software or sites-in-a-box: There are lots of opportunities to build tools and applications around data protection. Consumers need a way to manage the data about themselves, including passwords, personal information, transaction records and the like. Data gatherers need a way to tag data so they know what they can re-use, under what conditions, and what they must delete after a certain time or after, say, a bill is paid. There are huge opportunities in serving both sides of the market.

If you’re Esther Dyson: Publish a newsletter; write a book. Hold a conference. Publish on the Web. Use your bully pulpit to promote the idea of self-organizing governance systems. Because your organization is so small, you have a chance to promote the market without looking like a shill for “money-grubbing marketers.”

If you’re a customer: Educate yourself. Stick up for your rights, and go to merchants whose practices you like. Let them know that that’s what you’re doing. Remember that freedom of choice implies obligation to choose, and choose wisely.

If you’re anyone else: Guess our data-mining tools haven’t found you yet. If you run or own a Website, get cracking and develop data-management procedures, get your accounting firm to audit them, and post a disclosure statement on your site. Once you’ve gone to all that trouble, you might as well sign up with TRUSTe, because the license is the easy part. If you offer a business-to-business service, encourage your partners, clients, resellers or whatever to sign up with TRUSTe. Market the dickens out of your enlightened privacy policies. Let your Congresperson and the press know what you’re doing.
PERSONAL PRIVACY AND DATA CONTROL

Who should govern the use of individuals' data? Should it not be the individuals themselves?

Not everyone thinks so. Mailing houses, list managers and database companies think they own such data, and don't like to discuss what they do with it. Many governments and privacy advocates think it should be regulated tightly and its use controlled by law. And some people think that their personal history of payment defaults or auto accidents should be no of concern to anyone else.

Consumers are concerned, but for most of them it's a side issue, and no one has (until recently) had a vested interest in educating them. Their behavior often looks irrational because it's uninformed. Surveys show that fear of losing personal privacy is keeping consumers off the Net, yet people on the Net seem extremely careless with their own personal data. They worry about strangers getting hold of their personal details, yet they willingly fill out detailed questionnaires in hopes of winning a two-week vacation in Malaga or a 5-percent discount on a political magazine subscription. Then they get upset when someone offers them a special airfare (since they did not win the free trip) or asks for a contribution to the cause.

One reason for these contradictions is that it does not occur to most people that they might have a say in such matters. To the contrary, we believe that what happens to data should be up for negotiation between the parties to a transaction that generates the data. That is likely to happen, with lurches, on the Net. The next challenge will be to make it happen off the Net.

But first, we need to make a few distinctions.

Commercial data - and exclusions

The discussion here is about commercial data, supplied without coercion by individuals who are free to abandon a site or transaction. This starts with the kind of data generated in a transaction, where the customer and the merchant have the right to negotiate about the use of the data generated. Another source of data is simply the customer's behavior without an explicit transaction: what pages he visits, what he searches for, how he responds to banner ads.

The information we're discussing and the possibility of negotiation are mostly specific to the Net for now. As indicated on page 29, however, Net practices and attitudes are trickling back to influence treatment of the data on mass mailing lists. However they might have collected the information on their mailing lists, the member organizations of the Direct Marketing Association will de facto be forced to observe at least some of the rules that apply to Net-generated data as the DMA makes its privacy guidelines mandatory.

But we are not discussing information gleaned from discussion groups or news items on the Net and used in other ways, such as by a reporter, an employer (some laws sometimes apply), a prospective romantic partner or your school friends.
Moreover, privacy considerations change nature when someone makes promises: For example, a candidate for public office, with power over others and over public resources, has a limited right to privacy. Likewise, someone who wants a loan or an apartment or some other consideration has an obligation to reveal relevant information about a credit history, drum-practice hours or the like - or to offer a guarantee from some trusted third party who has access to that information. (We covered these issues at length in Release 1.0, 2-97, and also in our book, Release 2.0.)

Ultimately, banks may well take on the role of data banks, managing data on behalf of its owners and making various representations for them. Other potential players include certificate authorities such as VeriSign (page 24), and database firms and mailing houses themselves, if they can change their notion of who their ultimate customers are.

Finally, the rules should be different for data that is required by a government or other monopoly. Indeed, people in general are far more worried about the Internal Revenue Service than they are about Lands End or Amazon.com... and we hope the government keeps that in mind when it assesses progress come July. The power of monopolies such as governments should be constrained and the use of the data collected limited, by the same jurisdiction that allows the collector to demand the information in the first place. For example, like the information required in tax returns, information for drivers' licenses and the like should not be available to the public. Medical information is likewise a special category.

In short, the release of data to the government or to medical organizations, and by children, is usually not negotiated by individuals, and therefore strong legal protections should apply.

Privacy versus control of data

Privacy is a personal thing: What Juan considers privacy, Alice may consider isolation. Some people discuss their sexual habits freely but consider their salaries off-bounds; others feel the opposite. We like Delta to know how much we fly, because we get better service that way, but we're not sure we want them to keep a record of the movies we watch on board (after telling everyone that we need an on-board power supply so we can work non-stop!).

Some information we choose to keep private. And, which is more of a challenge, some information we'd like to release only to some people, with confidence that it will go no further.

That - control of the information once it leaves the individual's hands - is what this issue is all about. If corporations can control the use of content legally, why shouldn't individuals be able to control the use of data legally? Of course, there will always be breaches, inefficiencies and glitches, but the principle of control of data is hardly exceptionable. (The record-keeping technology to control data use already exists; it is just being used in behalf of the wrong players.)
Why we care

You might think that because the focus here is limited (or narrowed) to marketing data, that this kind of information is not very sensitive. But it can be - and combinations of it especially so.

"Consider how this would play out with a restaurant analogy," says Tara Lemmey, founder of Narrowline and a TRUSTe board member. "If you order food in one restaurant and pay by credit card, you do not assume another restaurant will know when you walk in what you ordered in the last and start making it for you. Nor do they have a copy of your card on file, or seat you next to other patrons you may have something in common with because a waiter heard your conversation and felt you would have an affinity for these folks. On the Net this happens now without an alert [often with data collected from cookies, the software that watches you as you Web-surf unless you turn it off]."

If you look at a site for AIDS care, do insurance companies redline your record (and avoid marketing to you)? Are you worried that if you visit the Communist Party site your employer may somehow find out?

Once individuals feel that they control their own data, many of the fuzzier questions about that ineffable thing called privacy will lose their bite. People will feel secure and worry less about what is known about them - because they'll know what it is. Those who really want to keep most information about themselves secret will be able to do so, using technology as well as contract law and regulations. The biggest challenge right now is ignorance: People aren’t worried enough, and are careless. Other people are worried too much, and are paranoid. No one knows what is known and what isn’t. It’s the one-way mirror effect that makes people so uneasy.

"There’s a fine line between good service and stalking."
- Tara Lemmey, Narrowline

Technology follows the user’s bidding

Managing all this data is a complicated matter. What makes the data interesting is often not a single item, but the correlations and compilations of data across collectors and databases. Technology, notably data-mining, allows people to find interesting patterns and predict behavior: Who’s likely to default on a loan? Buy life insurance? Refinance their home? Which of a site’s visitors spend the most at other sites, and on what? Does behavior online correspond with subsequent purchases? People interested in these questions generally have little interest in any individual’s personal life, but the data they collect, distributed elsewhere, could indeed invade someone’s privacy by almost anyone’s standards.

Meanwhile, more and more of people’s behavior can easily be recorded, from purchase patterns and reading habits to game-playing behavior and semi-public statements in online venues. The tools to collect and manipulate all this information have great power. The World Wide Web Consortium’s P3P (Platform for Privacy Preferences) lets users define and manage their personal data, and also provides a way for them to express how they want it used or restricted. But it also makes it easier for websites, servers and database managers to aggregate, manipulate, distribute, trade or sell such data.
Fortunately, those same powers can also be applied to controlling the use of the data, tagging it with restrictions on how it can be used or to whom it can be released. It can be encrypted with the keys restricted to specific third parties, or only to the creator(s) of the information. Individuals can also use P3P-compliant tools to express the conditions under which they will release data, and how it must be managed.

Of course, some privacy advocates feel that because such technology can be misused, it is better off not being developed at all. They have some justification, given a long history of privacy abuses around the world. The same technology that empowers individuals (and the providers of the personal data) also empowers large organizations who use the data and other individuals who might somehow get access to it.

A better solution is to encourage development of the technology, and discourage misuse of it. As with filtering tools, the same technology used by an individual for control can be used by a government for control over others - but blame the abuser, not the tool. Since the technology is there, we're glad companies are finally figuring out how to make it usable by normal people.

**THE CURRENT SITUATION AND A SCENARIO**

Businesses should want to overcome user fears in order to get more people online and buying things. But their lawyers tell them that making any promises about protecting customers' data would only expose them to liability. So even companies that do respect people's privacy end up not promoting that fact. They don't want to take on extra liability while other companies ignore the whole issue.

Meanwhile, privacy protection on the Net is a global issue. US Websites serve overseas consumers; overseas Websites serve US consumers. The US government and US businesses are responding to local pressures, but they are also concerned about the European Union's Data Protection Directive, slated to take effect in October. It is helping to push US activity along.

Within Europe it will ultimately force some coherence among the data-protection laws of its member states, but it could also cut Europe off from the rest of the world - or vice versa. In short, it will restrict access to European consumers by people or groups who don't comply with some fairly strict conditions for data protection, most of them set by law rather than specified or selected by the individuals involved.

Let a hundred jurisdictions bloom

Don't all the privacy rules need to be harmonized? Not really. Let it be up to the users (or voluntary groups of them) to decide under which jurisdiction they want to operate.

What's needed would simply be a labeling system, much like the ones various people and authorities are proposing for content (see Release 1.0, 12-96), and enabled by P3P among other technologies. That would let people make up their own minds. The labels could be as simple as, "This site follows French privacy laws," and French citizens who wanted their government's protection could restrict themselves to such sites. The US version would probably be more complex, with a label that says: "We observe the follow-
ing data protection policies. And we are liable under US law if we break our word." A similar approach could work for each other country.

You could also add non-state regimes or jurisdictions to the mix, as in the US example above. Much as the US is hoping to get the EU to say in effect: "We recognize the US laws as fulfilling our requirements," it could also say: "We recognize the rules of TRUSTe [or of hypothetical American Express merchant authorization requirements, or a given Big-Six/Four data-protection audit] as fulfilling our requirements."

That would foster a desirable outcome: a competitive market for government regulations - albeit one originally skewed by geography. That is, any customer could take into account a site's clearly-stated data-protection policies (whether voluntary or set by a government), just as she considers its prices, return policies and of course the products and prices it offers. Governments that had rules that didn't satisfy customers would find fewer and fewer people conducting business under their rules. Though they might not lose citizens, these governments (and their business-operating voters) would lose transactions.

This approach to data protection - coordinated rather than centralized - is not entirely a fantasy, although it would take unlikely amounts of common sense on all sides for it to happen quickly or even smoothly. It is de facto happening to a small extent in Europe in that each country has its own laws and they will be close enough (as rewritten under the directive) for each EU government to recognize their sufficiency. Of course the simplest way to handle conflicting laws is for each country to forbid foreign vendors to sell to its citizens. (When we enter a US airport, we see a sign telling us that the Nairobi airport does not follow US safety rules, and we are on our own if that's where we're headed.) Of course, that seems a little crazy, but so are all these conflicting rules. The EU's directive provides a sort of overall hurdle that each country must conform to.

Making it work: Wake up the sleeping dogs!

Meanwhile, the US the government is trying to forestall regulation and says it needs to be satisfied with industry's behavior vis a vis privacy.

More important, we believe, is the issue of customer behavior (which of course is influenced by market behavior). The industry can't create a market without informed customers who also play their role. Customers need to understand their own powers and change their behavior, becoming active players in a market for privacy by choice. In essence, the industry and government need to educate consumers to play their part, or consumers will get privacy as a "gift" in a form they may not want.

The industry needs to get active quickly in positioning personal data control as something both desirable and achievable. That will lure other vendors onto the bandwagon and make solutions visible along with problems.

Rosy scenario

The ideal scenario would be for the emerging solutions to satisfy the government, the public and privacy advocates. The most likely scenario is that a number of visible efforts will raise awareness, but actual compliance will still be "too low" by government standards. The government will pass some kind of disclosure law, without mandating the particular prac-
tices that must be disclosed (except perhaps vis a vis children). That would be a reasonable resolution and would spur the kind of activity we'd like to see.

Auditing firms will get into the act. Netscape and Microsoft will put privacy-disclosure-detection applets in their browsers, and users will be notified of the presence or absence of a disclosure statement. It would be illegal for a US-based site to lack one; the competitive pressures would then force many offshore sites to have one too.

Meanwhile, the European Union will look carefully at all this, consider the likelihood of reconciling things any other way, and enter into an understanding with the US government that its policies constitute compliance with the EU privacy directive.

Back to reality

There, that fantasy is simple! Let's explore the details.

While the government is planning conferences and hearings to assess the industry's progress since last July's announcement of the Framework for Global Electronic Commerce, the industry is busily coming up with a variety of approaches to customer data control. Notable are Microsoft's acquisition of Firefly, the forthcoming launch into the public domain of the World Wide Web Consortium's P3P technology, developments with TRUSTe and VeriSign, and a variety of initiatives by the American Institute of Certified Public Accountants, the Council of Better Business Bureaus, the Interactive Services Association, the Direct Marketing Association, the Internet Content Coalition (supporting TRUSTe) and others. Various privacy advocates are calling for regulation. The Aspen Institute has started the Internet Policy Project under the able directorship of Counsel Connect founder and legal scholar David Johnson (Release 1.0, 6-96) to look at how self-governance without regulation can emerge, with privacy as one of several test cases. IBM is promoting a Consumer Privacy Initiative and is hosting its own privacy conference (sponsored by its Institute for Advanced Commerce) for corporate customers in May, and, as one of the industry's largest and most global firms, quietly lobbying the European governments. Here with a round-up.

"Do we really want to mandate that everyone who sets up a Website - including individuals and small publishing operations - must install what to them would be a costly auditing process? This might approximate trying to regulate what you can do with what you learn at a dinner party. It's not much comfort to assume that most laws won't be effectively enforced against small players, because unenforced laws reduce confidence in the legal system overall. Rather, we might better either look to voluntary leadership by large players or limit any regulatory requirements to the relatively few large institutions that can readily bear the costs."

- David Johnson, Aspen Institute
But first, a message from the government....

Elements of Effective Self-Regulation for Protection of Privacy
A draft document from the Department of Commerce

As set forth in A Framework for Global Electronic Commerce, the Clinton Administration supports private sector efforts to implement meaningful, consumer-friendly, self-regulatory regimes to protect privacy. To be meaningful, self-regulation must do more than articulate broad policies or guidelines. Effective self-regulation involves substantive rules, as well as the means to ensure that consumers know the rules, that companies comply with them, and that consumers have appropriate recourse when injuries result from noncompliance. This paper discusses the elements of effective self-regulatory regimes—elements that incorporate principles of fair information practices with enforcement mechanisms that assure compliance with those practices.

A. Principles of Fair Information Practices

Fair information practices were originally identified by an advisory committee of the U.S. Department of Health Education and Welfare in 1973 and form the basis for the Privacy Act of 1974, the legislation that protects personal information collected and maintained by the United States government. These principles were later adopted by the international community in the Organization for Economic Cooperation and Development's Guidelines for the Protection of Personal Data and Transborder Data Flows. Principles of fair information practices include consumer awareness, choice, appropriate levels of security, and consumer access to their personally identifiable data. While the discussion that follows suggests ways in which these principles can be implemented, the private sector is encouraged to develop its own ways of accomplishing this goal.

1. Awareness. At a minimum, consumers need to know the identity of the collector of their personal information, the intended uses of the information, and the means by which they may limit its disclosure. Companies collecting and using data are responsible for raising consumer awareness and can do so through the following avenues:

- Privacy policies. Privacy policies articulate the manner in which a company collects, uses, and protects data, and the choices they offer consumers to exercise rights in their personal information is used. On the basis of this policy, consumers can determine whether and to what extent they wish to make information available to companies.

- Notification. A company's privacy policy should be made known to consumers. Notification should be written in language that is clear and easily understood, should be displayed prominently, and should be made available before consumers are asked to relinquish information to the company.
Consumer education. Companies should teach consumers to ask for relevant knowledge about why information is being collected, what the information will be used for, how it will be protected, the consequences of providing or withholding information, and any recourse they may have. Consumer education enables consumers to make informed decisions about how they allow their personal data to be used as they participate in the information economy. Consumer education may be carried out by individual companies, trade associations, or industry public service campaigns.

2. Choice. Consumers should be given the opportunity to exercise choice with respect to whether and how their personal information is used, either by businesses with whom they have direct contact or by third parties. Consumers should be provided with simple, readily visible, available, and affordable mechanisms — whether through technological means or otherwise — to exercise this option. For certain kinds of information, e.g., medical information or information related to children, affirmative choice by consumers may be appropriate. In these cases, companies should not use personal information unless its use is explicitly consented to by the individual or, in the case of children, his or her parent or guardian.

3. Data Security. Companies creating, maintaining, using or disseminating records of identifiable personal information should take reasonable measures to assure its reliability for its intended use and should take reasonable precautions to protect it from loss, misuse, alteration or destruction. Companies should also strive to assure that the level of protection extended by third parties to whom they transfer personal information is at a level comparable to its own.

4. Consumer Access. Consumers should have the opportunity for reasonable, appropriate access to information about them that a company holds, and be able to correct or amend that information when necessary. The extent of access may vary from industry to industry. Providing access to consumer information can be costly to companies, and thus decisions about the level of appropriate access should take into account the nature of the information collected, the number of locations in which it is stored, the nature of the enterprise, and the ways in which the information is to be used.

B. Enforcement.

To be effective, a self-regulatory privacy regime should include mechanisms to assure compliance with the rules and appropriate recourse to an injured party when rules are not followed. Such mechanisms are essential tools to enable consumers to exercise their privacy rights, and should, therefore, be readily available and affordable to consumers. They may take several forms, as proposed below, and businesses may need to use more than one depending upon the nature of the enterprise and the kind of information the company collects and uses. The discussion of enforcement tools below is in no way intended to be limiting. The private sector may design the means to provide enforcement that best suit its needs and the needs of consumers.
THE STORY SO FAR

It all began gloriously last July 2, when Bill Clinton and Al Gore stood up and talked about the promise and potential of the Internet for the American people. They unveiled the Framework for Global Electronic Commerce, and IBM's Lou Gerstner said a few words. The Communications Decency Act had recently been overturned, and the future looked bright. Government's first rule for the Internet, said Vice President Gore, should be “do no harm.” There were mutterings about privacy, spamming and the like, but the government, with strong guidance from Ira Magaziner, decided to let the industry see what it could come up with.

A year later, not much has happened on the privacy front, although e-commerce is booming. Privacy concerns may be a constraint on consumer acceptance, but businesses aren't seeing the customers they're missing.

However, though the furor over spamming has somewhat died down, the problem hasn't, while the furor over privacy is building. A number of private polls have convinced the government that it needs to do something: The people of America are concerned about their privacy (or can be incited to it by pressure groups) and would like the government to solve the problem.

The question is: How to turn the public's imagination to a better solution — not government regulation or even industry self-regulation, but an environment where consumers themselves can exercise their power and control.

1. Consumer recourse. Companies that collect and use personally identifiable information should offer consumers mechanisms by which their complaints can be resolved. Such mechanisms should be readily available and affordable.

2. Verification. Verification provides attestation that the assertions businesses make about their privacy practices are true and that privacy practices have been implemented as represented. The nature and the extent of verification depends upon the kind of information with which a company deals — companies using highly sensitive information may be held to a higher standard of verification. Because verification may be costly for business, work needs to be done to arrive at appropriate, cost-effective ways to provide companies with the means to provide verification.

3. Consequences. For self-regulation to be effective, failure to comply with fair information practices should have consequences. Among these may be cancellation of the right to use a certifying seal or logo, posting the name of the non-complier on a publicly available "bad-actor" list, or disqualification from membership in an industry trade association. Non-compliers could be required to pay the costs of determining their non-compliance. Ultimately, sanctions should be stiff enough to be meaningful and swift enough to assure consumers that their concerns are addressed in a timely fashion. When companies make assertions that they are abiding by certain privacy practices and then fail to do so, they may be liable for fraud and subject to action by the Federal Trade Commission.

Release 1.0 23 April 1998
their own data? So far, no one has been telling them that this is possible, and so they look to the government as the obvious answer.

The situation now, part 2

Now, as of mid-April, we’re left with the looming question: Can the market of its own accord come up with credible responses by the one-year-anniversary deadline? Here’s the line-up now.

Since January, Internet czar Ira Magaziner and Commerce Secretary William Daley have been visiting industry leaders, laying out the situation above. Magaziner has also been touring the globe, trying to persuade other countries that the market will come up with a solution, and can’t we all work together?

The Federal Trade Commission will report to Congress in July on a survey of Websites and existing industry guidelines and policies. The Department of Commerce will hold a privacy summit preview on May 13 to 14 and co-sponsor a privacy summit with the White House in June. The Administration’s goal is to highlight the market’s solutions. If there isn’t enough to highlight, the Administration will probably propose some legislation in July.

On the “industry” side, of course, there is no industry as such. There are a lot of players, most of them lacking much sense of urgency until recently. (What word is it that they don’t understand in the phrase: “Legislation in July unless there’s a credible solution”?)

But finally things are starting to come together. Despite confusion, political angst and the like, trade associations and other groups are starting to weigh in, as are big players including IBM, HP and Microsoft. The Direct Marketing Association is taking the issue seriously. Ideally, everyone should converge on TRUSTe, not as the single guarantor of privacy, but as the best example and a model for a host of future competitors. On the accounting side, the American Institute of Certified Public Accountants is promoting the WebTrust assurance program, which covers “information protection” among other items. The Council of Better Business Bureaus has a plan to add privacy assurance to its services through BBBOnline.

Missing in action are the legal professions and the insurance industry, all of which should be bringing their people and their methodologies to bear. For this is not a technical question only; it concerns guarantees, representations, auditing, risks, compliance...and liability.

! NEWS FLASH! MICROSOFT ACQUIRES FIREFLY

Earlier this month Microsoft acquired Firefly (see Release 1.0, 2-97 and 11-96, and disclosure, page 2). Firefly is a leader in implementing tools and systems for users to express their own privacy preferences and manage their own personal data. It developed some of the underlying data management technology in a joint effort with Netscape and VeriSign, which the group then donated to the World Wide Web Consortium (W3C), where it was incorporated into a broader suite of protocols under the name P3P (Platform for Privacy Preferences). Obviously, the value in the acquisition is not the technology itself, which is in the public domain, but Firefly’s expertise in using it and the company’s understanding of the issues involved.
Nothing is guaranteed, but if Microsoft leads an industry movement for personal data control, that could make for big changes in popular perception and attention to the issue. Microsoft's moves, of course, are complicated by its delicate relations with Washington overall currently, but presenting itself as an empowerer of consumers has to be a good thing for me and everyone else.

The key is that the company should continue to cooperate with other industry players (including Netscape), in addition to working through the W3C or other "public" standards groups. Ideally, the technology should reside in Windows rather than just in the browser (and on other platforms as well, to be sure!). That is, if Microsoft removes Internet Explorer, the technology should still be there, although the IE interface to it would be Microsoft's own proprietary technology. Other browsers and user tools could also address it.

"Where do you want your data today?"

Whatever you may think of Microsoft's ultimate intentions, it has built a solid business on empowering its customers as individuals. Of course it understands the allure of cookies and vendor-side data-collection, and its corporate nature may be to want control of everything. But as a technology provider it is firmly on the client side, despite its own occasional efforts to look corporate. Says Ed Jung, General Manager, Web Platforms of the Web Essentials Group: "A lot of the technology out there to support privacy is pretty thin. Privacy is something users want, but they don't want to deal with all the UI of it. We hope to come up with something pretty decent, some technology to make it palatable to users. We want to work with sites to make sure the policies they come up with are reasonable. Hopefully we can build enough of a network effect to get people to line up for it."

For now, Firefly will join Microsoft's Web Essentials group, positioning it as part of content and tools rather than as a platform technology. But Microsoft re-orgs enough that that doesn't mean too much. The acquisition has high-level visibility within Microsoft.

Acquiring a technology and a conscience

What does Firefly bring to the party? First of all, Microsoft is acquiring Nick Grouf, Firefly's CEO - call him a privacy conscience. Of course, we've all seen acquisitions where the people and the technology vanish without a trace, but there are also exceptions. Microsoft CTO Nathan Myhrvold was "acquired" along with Dynamical Systems, which was acquired for some of the graphics expertise that made its way into Windows. Myhrvold is now a key part of Microsoft's personality just as graphics is a key part of Windows.

Grouf plans to move to Redmond and stay actively involved. Firefly right now has some technology for data management and data representation, in addition to the technology it donated to the World Wide Web Consortium. That public-domain technology, P3P, is now managed by W3C and is soon to be released as a formal specification; Microsoft/Firefly will be demoing it on behalf of W3C at the forthcoming Department of Commerce show&tell. But the specific implementations, expertise and attitudes, embodied in 70 people who have all been invited to Redmond, comprise the value-added that makes the acquisition exciting. On the server side, Firefly has expertise and
experience in medium-range scaling-up of data management. (Firefly's much-hailed collaborative filtering technology is of less interest to Microsoft.)

For those who are skeptical, note that the rumored acquisition price for Firefly was less than a tenth of the rumored $400 million that Microsoft recently paid for HotMail and its 10 million e-mail users. One reason, we're sure, is that Microsoft doesn't automatically get access to Firefly's 3 million-odd customers. Each of them will be invited individually to come to the Firefly/Microsoft Website and re-register if he or she wants to keep an account (and data) with Microsoft. (In privacy parlance, that's known as opt-in, a stronger protection than opt-out, where the user's data is retained unless directed otherwise.)

Microsoft clearly has the capability to promote the concept of user data control as a worthwhile consumer benefit. It also has the incentive to do so, for the government is breathing down no neck more than Microsoft's.

What it doesn't have is the social and legal infrastructure on the other side. Indeed, to the extent that it uses Firefly technology in its own content services, it too will face the tougher questions that bedevil Website managers and data collectors overall: actually defining a policy, getting audited, making a disclosure statement, and so forth. (That will be a good product-testing exercise, if nothing else!)

"Individual users should be confident in using these technologies, and security and privacy are a big part of that."

- Bob Herbold, Microsoft

THE US GOVERNMENT: GOOD COPS AND BAD COPS

The US Government is now in a slightly embarrassing position. It has told both the US public and a variety of foreign governments to hold on: The Net can govern itself. Now those cheerful assurances are fading, as little has happened since the summit last year. Says Ira Magaziner: "Our hope is that by mid-May there'll be something that can be announced. If there's nothing by July 1, we'll need to go to plan B."

He continues: "The issue is going to come to a head pretty soon. We're on a knife's edge. The public is concerned. But even if we passed a thousand pages of airtight laws, there's no way we could enforce them. The private sector should come up with codes of conduct, notice and consent. We need organizations with seals that a Website can display and some enforcement and auditing mechanisms. The basic model is very close to TRUSTe. Then there's the normal backup of the FTC or a foreign equivalent if there's fraud in the representations. This approach makes it easier to go international: You could use the same seal with different enforcers - TRUSTe, governments, whatever."

The Department of Commerce is working closely with the Administration on all this, while the Federal Trade Commission is answerable more directly to Congress. Each must deliver a report to its overseer in late June/early July. The reports will probably contain news of inadequacies coupled with many promised remedies.
The greatest sticking point, aside from a lack of operational recourse mechanisms for consumers, is likely to be disclosure not of privacy policies but of individual data to the individuals themselves. That is, letting Juan know what’s in his record so he can correct it. Companies will always promise recourse to injured individuals because they don’t plan to injure anyone, but they are loath to assume the burden of setting up adequately staffed hotlines or other facilities to deal with consumer questions about their own data. (Just ask the Social Security Administration what a challenge that can be!)

This is a legitimate concern; as we all know, dealing with consumers is expensive. But if you’re willing to talk to Juan when he wants to buy, you should be willing to talk to him when he has an honest question. It’s the “you-first” problem: No company wants to bear such costs if its competitors don’t have to.

Of course, if consumers start taking control of their own data, encrypting in and sending it to third parties of their own choice for safekeeping as VeriSign suggests (page 24), vendors won’t have to deal with this problem either.

“We need to go to consumers with an education campaign.”
- Ira Magaziner, the White House

The Department of Commerce

The Department of Commerce is encouraging industry to demonstrate its solutions to privacy problems and promoting its efforts to the public. More unabashedly pro-business than the FTC, the DOC is sponsoring a couple of conferences for the “industry” to showcase its efforts. The first will be May 13 to 14, sort of a dress rehearsal, and the second, more public one, to be held jointly with the White House, will probably be in June. The Department of Commerce is also preparing a report to the Administration, which is due July 1.

As shown on pages 11 to 13, the DOC has published for comments a draft “self-regulation of privacy elements” paper both on the Net and in the Federal Register. It hopes to get input before the conference and also for its report. The paper describes the “elements” of Fair Information Practices, including awareness, choice, data security and consumer access, and enforcement. Enforcement, the stickiest one, includes consumer recourse, verification and consequences, internal mechanisms for implementing company privacy policies, and third-party verification and dispute resolution mechanisms.

The DOC’s conference will include consideration of proposed methodologies for assessing compliance with the Department’s Elements Paper. It will also feature technology demonstrations and service presentations along with discussions of the merits and inadequacies of various approaches. And it will include workshops for specific markets/sectors, such as financial services, children’s sites, Internet access and content providers. Much of the outside coordination work for the conference, including management of the mailing list, is being handled by CDT.
Given that one significant part of the problem is lack of public awareness, this conference and its White House successor could be of real value in drawing attention to both problems and solutions.

The Federal Trade Commission

“This is our report card, and if the grades aren't good...”

David Medine, FTC

The DOC and Federal Trade Commission’s overall positions are fairly consistent; the difference is more in attitude to what is actually happening. The FTC, which has been working this issue the longest, is the more impatient. It began very hands-off, when it first considered “Net privacy” at the behest of then-Commissioner Christine Varney in April 1995. But the Commission has been frustrated with the lack of action since, and so has Varney. (She is now a TRUSTe board member and working in private practice at Hogan & Hartson advising such companies as Netscape, Earthlink, IBM, Time-Warner, Disney and America Online. Can she get more of a hearing from these companies as clients?)

Like the DOC, the FTC is working on a report due in June, this one to the Congress. The FTC recently surveyed the marketplace, evaluating 1200 Websites, including the top 100 sites, 100 directed at children, and 1000 randomly selected. The criteria, similar to the DOC’s “Elements,” are notice, choice, auditing and recourse. It is also analyzing responses to a March 5 request for interested trade associations and industry groups to submit copies of their information practice guidelines and principles for inclusion in the report. The FTC won’t discuss the results so far, but word is that they are not encouraging.

On March 26, David Medine, Associate Director for Credit Practices of the FTC’s Bureau of Consumer Protection, bluntly warned before Congress: “The Commission supports technological innovation and also encourages industry self-regulation so long as self-regulation proves meaningful and effective. The upcoming June report...will shed light on how much progress self-regulation has made...If such progress is inadequate, appropriate alternatives may need to be explored.”

The private sector

“Hold tightly to the hand of Nurse, for fear of finding something worse.”

- Hillaire Belloc, poet

“A seal a day keeps the government away.”

- anonymous (not J. Klein)

TRUSTe: The Very Model of a Modern Major Monitor?

The great white hope of the movement is TRUSTe, a non-profit organization established in 1996 by the Electronic Frontier Foundation and Commercenet. [See disclosure on page 2.] TRUSTe, described at length in Release 1.0, 2-
197, initially failed to live up to its early promise; despite protestations of moral support, it won inadequate tangible support from industry. It raised $1 million in its first year, says founding chairman Lori Fena, but much of that was in advertising dollars, which can't pay staff for a hotline or beady-eyed site auditors.

Now TRUSTe is catching up rapidly, mostly because of government pressure that is "encouraging" companies to adopt a solution - any solution - in the face of impending regulation. Although officials are careful to praise the concept, not the particular vehicle, their message is clear and TRUSTe is one of the few alternatives. Other governments, including Australia, have mentioned TRUSTe by name with approval, if not with official endorsements. Some EU Parliament members are watching with interest.

In just the last few weeks, TRUSTe has won a rash of sign-ups, endorsements and the like, pushing the number of licensees to over 100, of which 50 are now up and running. Moreover, the licensees include 8 of the top 20 Websites, such as Excite, CNET, Disney, Wired's HotWired and so forth. Executive director Susan Scott is now going after the aggregators, encouraging them to encourage their "suppliers" to support TRUSTe. Can Netscape, Yahoo! and Time Warner be far behind?

Also last month, the Internet Content Coalition, an alliance of content providers, formally endorsed TRUSTe - a significant move, but one that is not binding on its members. ICC member CNET already has a TRUSTe license, and CNET editor and ICC chairman Chris Barr has editorialized in its favor. The New York Times on the Web and New York Today are working to get licensed. ICC board member and NYT Electronic Media Company president Martin Nisenholtz says, "I had very little trouble [internally] getting that done. We all recognized that this was an important thing to do. As far as the Times goes, the only concern would be not to involve the First Amendment. But it doesn't have anything to do with editorial coverage in the sense of interfering with the public's right to know or freedom of information."

Other members of the ICC include CBS Online, Playboy Enterprises, MSNBC, Sony Online, Time Inc., The Weather Channel, Warner Brothers online, Warner Music Group and ZDNet. Most of them already have some sort of privacy policy posted, but no mechanism for the other elements: validation and customer recourse. Says Scott, "They're the first association to step up and say this is the way the industry should go, that TRUSTe is the way to follow the Commerce guidelines. They should be applauded for stepping up. A lot of people are proposing privacy statements, but they understand that we need an oversight vehicle."

That's a welcome change. Previously, says Scott, "We'd talk to the marketing people and they'd want to do it, but then they'd go to the lawyers. The lawyers would say, 'Why sign ourselves up for a liability we don't have? We're safer just leaving this alone.'"

**Truth = trust?**

Now, the government is about to impose such a liability, and TRUSTe looks like a better choice. In fact, TRUSTe is extremely flexible: It's a standard for disclosure, a labeling system, and an auditing/recourse mechanism. But aside from some best-practices regarding children, it leaves licensees free to do what they want with their customers' data - as long as they disclose their practices and follow their promises.
That approach, however, is still under discussion by the organization's board. "We're also considering whether to adopt mandatory opt-in or opt-out," says TRUSTe board member and current EFF chairman Lori Fena. "We will go wherever the market, regulations and consumers lead us."

The original version of TRUSTe, with three different trustmarks, confused consumers. Critics complain that consumers should be able to trust a site with a "trustmark," rather than look for details. The implicit message of TRUSTe as it is now is that what happens to an individual's data is his responsibility; he shouldn't leave those decisions in someone else's hands. After all, consumers have learned to look for the lowest interest rate on their credit cards; they understand credit isn't free, and that they should check the fine print. What's different here?

From TRUSTe's Website...

The Trustmark — A Symbol of Trust

The TRUSTe trustmark signifies to users that a Web site is a TRUSTe licensee. As a licensee displaying the trustmark, you are sending a clear signal to users that you've agreed to disclose your information gathering and dissemination practices, and that disclosure is backed by third-party assurance. Each trustmark is linked to a licensee's unique privacy statement, which users can bring up by clicking on the mark.

Privacy Statements

As a TRUSTe licensee, you will display a trustmark on your home page that represents an overall privacy statement; i.e., the privacy practices that pertain to your entire site. Licensees also have the option of displaying a trustmark on other pages where personal information is collected. TRUSTe recommends this practice, as it allows licensees to reflect accurately the disclosure practices throughout their site (besides, users often enter a site at locations other than the home page). A trustmark not on the home page signifies a tailored privacy statement that pertains only to the privacy practices of the specific page or location where the trustmark is displayed.

Whether overall or tailored, each privacy statement discloses, at a minimum:

· What type of information the Web site gathers
· How the site uses the information
· Who the site shares information with
· Whether users can correct and update their personally identifiable information
· Whether users will be deleted or deactivated from the site's data base upon request
· Whether users may opt out of giving specific information to third parties
**Recourse mechanisms**

When there’s a problem, it could surface either through TRUSTe’s auditing or via a consumer complaint. First, TRUSTe sends off a formal notice and gives the target an opportunity to respond. If the response is inadequate, TRUSTe can pursue it according to contract - revoking the license and the mark, auditing the miscreant (at the licensee’s cost) and publicizing the results. If the breach appears willful and fraudulent, TRUSTe can call in the local jurisdiction under which the license was signed (usually a US court) and sue. TRUSTe can also call in the FTC or other government agencies in serious cases.

TRUSTe’s recourse mechanisms sound reasonable, but they haven’t really been tested yet. Notes Lori Fena, “Naturally enough, the first few hundred companies to sign up will tend to be the most sincere. We have contacted people [licensees] about what looked like problems. When you point something out, it’s an oversight and they want to clear it up.”

TRUSTe is now an old hand at the issues involved with customer data control, says Scott. For example, “I can’t tell you how many times we’ve had to call sites even after they’ve paid their fees. And there are other issues: We have technology that goes back and forth and checks the privacy statement to see if anything has changed. If a consumer complains, how can you prove what the privacy statement was on that date? We actively audit sites and check for breaches. We’re not just a middleman.”

**The challenges**

As a spur to action, TRUSTe negotiated a discount on the license fee with the ICC members. However, the TRUSTe fee is only a small part of the overall costs. The fee is $250 up; not everyone is audited, but are all subject to audit. For large sites, signing up for TRUSTe can mean an extensive overhaul/audit of internal data-management procedures. Worse, for large companies with small sites, it can mean tail wagging dog: Net data practices drive a change from long-established practices, since who wants to segregate Net-acquired data from what a company acquires elsewhere? (Of course, we’d argue that the overhaul may be a good thing, but it certainly increases the work a company must do to adopt TRUSTe or any other serious privacy measures.)

For small companies, there are problems too. Remember that the Net is a medium not just for corporate giants, but also for the amateur biscuit-maker, Di Caprio fan site, grade school, Daily Soup shop and DaveNet. For example, we have a friend who runs her company’s Website and receives all its e-mail in her spare time. “I don’t want to use anybody’s data; I don’t have time! But we’re collecting it, and I don’t want to promise what we might or might not do with it later,” she says. She looked at the build-your-own-statement tool on the DMA Website, but decided not to use it. “If people write and ask I tell them we’re not doing anything with their information, but I don’t want to post a general promise.”

Perhaps there’s a real opportunity here for site-in-a-box vendors such as BroadVision, Encanto, iCat (Esther Dyson is an investor) and Intershop, and software/service firms such as USWeb or Open Market, to include back-end data management and front-end privacy policies, but they will need to be fairly robust to work well. That is, if you modify the data-management features, it should be reflected in the privacy disclosure. Better yet,
Imagine if Visa or American Express were to make TRUSTe membership or something similar a condition for receipt of merchant authorization!

It doesn't seem unreasonable for people to manage customer data as carefully as they manage money. Automation, after all, does make both tasks easier. Besides, you can always disclose as follows: “For now, we're keeping your data in a virtual shoebox, and we reserve the right to use it in any way later.”

"Here it is 11:59 pm, and people are saying omigosh!"

- Susan Scott, TRUSTe

WEBTRUST FROM THE AICPA: PRIVACY AS PART OF A PACKAGE

The accounting industry has long wondered what accounting firms can do in addition to auditing a company’s financial statements. There are lots of answers; just ask Andersen! The American Institute of Certified Public Accountants, the accounting industry's major group, has another answer: the WebTrust program, a set of assurance practices for commercial Websites certified by the WebTrust seal.

Although the program is focused on commercial sites right now (after all, those are the sites most likely to need an accounting firm in the first place) there's no reason that the WebTrust program couldn't apply to non-transaction sites too in the long run. Many of them also keep books, and they need validated data to show to advertisers, sponsors or whoever is paying the bills.

The WebTrust principles concern business practices disclosure and transaction integrity as well as privacy, or what the AICPA calls “information protection.” The AICPA Website, in fact, contains great volumes of information and a useful checklist for anyone contemplating offering goods or services online.

So far, the AICPA has awarded three seals (one to the AICPA itself) since serious marketing started last month. It takes time to be audited! Training of the CPAs started last year, and 65 accounting firms are now certified to perform the WebTrust audits. In case you want to know, the first outside licensees are Creativekids.com, which sells educational toys and software, and Resource-marketing.com, which offers Web-hosting services.

Other sites are currently being reviewed by their auditors. The AICPA has launched a broad advertising campaign in the consumer and trade press to create awareness among consumers and Webmasters alike. It is also leveraging its membership of 330,000 CPAs in the US and extending the program to Canada.

Sorry, not my fault

The problem with the WebTrust program is that it has no formal procedures for recourse and accountability - which of course is a hot issue among accountants generally. Revocation is the sole remedy for non-compliance, although complaints can be forwarded to the certifying auditor. For obvious reasons, the accountants want to avoid assuming liability upfront. The AICPA seems to be relying on the general notion that if an accounting firm has too many crooked clients the AICPA will investigate - or the courts

Release 1.0 23 April 1998
that is true in the long run, but it may or may not impress folks inside and outside the government who want genuine recourse and accountability. "We’re always evaluating what makes the most sense. In the software model, we’re just at Release 1.0," says K. Casey Bennett, AICPA’s director of assurance services for the AICPA. He led the committee of a dozen people who worked on the program.

The other main objection we have heard to WebTrust is that it’s more a marketing program for CPAs and too expensive for small sites. Among other things, the sites need to be re-certified by an auditor each 90 days. As the AICPA’s FAQ for practitioners delicately notes: “This service will also position a firm for opportunities which are emerging with the rapid change of technology as well as afford some protection from the eroding of other more traditional service lines caused by this change in technology.”

We think the basic understanding has to change. Privacy is expensive, and it is a marketing opportunity. Yes, it’s cheap to set up your own Website and have a simple disclosure statement that says: “We don’t collect data except for our own use, to communicate with you directly. For any other use, we will contact you to ask your permission.”

But for any site that wants to do more, the systems are costly, and so are the assurance mechanisms. Hey, it’s costly to get audited, to keep financial statements, to pay taxes, to monitor usage patterns and demographics to sell ads.

“As we say to industry, if you think this costs you money and effort to organize, it’s a lot cheaper than the alternative. You’ll have it anyway, but if you have it through a government privacy board, it won’t be as flexible. They’re beginning to recognize we’re serious.”

– Ira Magaziner – The White House

BBBONLINE: OMNI PRESENT

The Council of Better Business Bureaus has developed a proposal to make privacy assurance a service offered through its subsidiary BBBOnline. It does not yet have the appropriate mechanisms in place, and it won’t go ahead to develop them without an assurance of funding, which it is currently working on. See also page 14. (BBB approached TRUSTe with an offer to merge, but that idea seems to have been abandoned. We don’t particularly care for this idea, and in fact we’d like to see both TRUSTe and BBB continuing to operate independently, broadening the “privacy market” instead of consolidating.)

What BBBOnline does have is its connection to the BBB and a broad network of members, support staff, dispute resolution people, and a brand name - in the US at least. The original Better Business Bureau was founded 80 years ago, and the nationwide Council of BBBs was formed in 1981 by a consortium of major corporations. Its basic mission is to support truth in advertising; accordingly, if you consider advertising of your privacy practices, it fits right in.

The Council’s National Advertising Division has handled 3000 advertising disputes between major companies, with 98 percent satisfaction, says Russ Bodoff, vp and general manager of BBBOnline. And its Children’s Advertis
ing Review Unit is the acknowledged leader in that space, and is the locus of the Council's privacy efforts so far.

Two years ago, the Council set up BBBOnline to help consumers identify reliable businesses on Net. Its board comprises Ameritech, AT&T, Eastman Kodak, GTE, HP, Netscape, Time Warner, Sony Electronics, US West, Visa and Xerox. It has certified 1200 Websites nationwide.

The BBB does not yet have the auditing and recourse functions TRUSTe has painstakingly constructed. By all means, it should build them rather than absorbing those of TRUSTe. Meanwhile, TRUSTe should build its own dispute resolution infrastructure. Then, in a year or two, TRUSTe will have some healthy competition.

**VERISIGN: TECHNOLOGIES FOR TRUST**

TRUSTe is a system for disclosing privacy policies and overseeing them in practice through social and legal means. But when you visit a Website, how can you be sure it really is certified by TRUSTe, AICPA or whatever? VeriSign has signed up the AICPA and is now working on an agreement with TRUSTe to certify the identity and authorization of TRUSTe Websites.

VeriSign offers a special AICPA-enabled Digital ID which will enable Website visitors to examine the Digital ID and assure themselves that the site is truly certified by an AICPA member or is a TRUSTe member and isn't just making the claim. The ID is indicated by a joint seal which, when clicked, goes into SSL-enabled mode on the site and explains to the user how to examine the Digital ID. Of course, the two different "brands" of IDs have subtly different meanings.

Additionally, TRUSTe and VeriSign are working together to try to sign up the top 20 commercial Websites in time for the Department of Commerce's Privacy Summit in May. "We wanted to have a real solution available now with the leading sites signed up for something real, so we're leading with Website Privacy Policy disclosure through TRUSTe and VeriSign," says VeriSign's Greg Smirin, director of Internet product marketing.

Simultaneously, TRUSTe and VeriSign are trying to get the browser vendors to add a feature that would inspect for the presence or absence of a privacy policy at a Website (as certified by VeriSign), much like the Netscape broken or closed key (now padlock) used to reflect a secure site. Recall that VeriSign was one several companies (along with Netscape and Firefly) that helped develop the P3P technology for the World Wide Web consortium, and you'll see how neatly this all hangs together.

As for VeriSign's other plans, it already offers digital certificates that can be anonymous (used today by Netscape's NetCenter). VeriSign is now exploring services which would allow users to surf anonymously, divulging information to sites on a selective basis. The customer would have a digital signature (a "Privacy Digital ID") with encrypted information on it. Keys to unlock specific items of information (name, say, but not social security or address or credit card number) would be available only to merchants or delivery services who meet certain qualifications and receive keys from some trusted third party. These Privacy Digital IDs would thus allow anonymous Website visitors to present their IDs to sites and allow those sites (who subscribed to a Privacy policy from TRUSTe or others) to either...
read masked information from that ID or to retrieve information from a network of trusted third parties who issue the Privacy IDs.

In the model with the ID acting as a pointer to an information service, you could send and receive e-mail, visit sites and transact business without divulging your identity to that site. Physical items could be sent to a third-party service that could resolve addresses using a secure database from VeriSign or other trusted third parties. Thus Amazon.com could sell a book to an unidentified buyer with a credit card number it never saw. It would ship the book to, say, Federal Express, which could decrypt the address and a name (not necessarily the real name) for shipping, without knowing (other than “books”) what was inside or who it was for.

Of course, that means consumers would have to trust VeriSign...or someone. Do you prefer a single point of failure, or distributed risk among many parties you don’t know? Of course, a single person could have multiple digital certificates for different slices of his life.

For those who don't trust anyone, there are further technical/physical means of protecting privacy. They range from the simple - don't tell anyone anything - to the complex. You can post through an anonymizer. You can get an e-mail account with a fake name through HotMail - no billing address needed, although your messages can be traced back to the machine(s) you use. You can (as such services becomes more widespread) pay for things with anonymous cash and have them sent to PO boxes. (Don't forget your mustache and sunglasses when you pick up the package!) Many people already use designates or proxies to represent them in various ways; in cyberspace, that, like so many intangible services, is likely to become a more broadly available facility. We expect that such services will find a market: Some people will use them some of the time, and a few people will use them all of the time.

IBM AND THE CONSUMER PRIVACY INITIATIVE

IBM has taken on privacy as a key issue for its e-business initiatives. The various parts of IBM are all involved, from Irving Wladawsky-Berger who runs the Internet group, to the public-policy group in Washington. IBM's Roger Cochetti (Internet Policy Director in Washington) sits on the board of TRUSTe. Senior vp & general counsel Lawrence Ricciardi recently updated the company's privacy policies. "We accept the premise of leadership," says Harriet Pearson, IBM public affairs director, and also in Washington. "Lou Gerstner feels we need to make good on that, both for the health of the Net and our customers, and for our own specific advantage. We need to think ahead of the curve."

Accordingly, IBM is organizing its own set of meetings to create what it calls the Consumer Privacy Initiative. "There's a need for an overarching alliance of committed companies, trade groups and consumers to address online privacy. We need powerful resources," says Pearson. "We hope that by convening some influential and credible players we can offer a more tangible and real manifestation of the issues. It's not just for the elites. We need something that goes out to the consumer, that visibly makes the Net a safer environment." As we have noted elsewhere, for the market to work consumers need to do their part, and they need to be educated in order to do so.
The goal is to create a cross-sector privacy alliance, says Pearson, whose functions would include yet another take on the four elements: ubiquitous support of fundamental privacy principles and practices; consumer education/outreach, including education on available technology tools and what to ask businesses about their data practices; so-called "business recruiting," or getting businesses to endorse and implement privacy protection; and verification, dispute-resolution and complaint-handling mechanisms.

IBM held the initial, organizing meeting of the Consumer Privacy Initiative in Washington on April 17, attracting about 50 of the usual suspects from a variety of the companies and organizations mentioned here and similar ones. Not a great deal was resolved but a sense of urgency was felt, and the next meeting is scheduled for April 24 - unusually fast for this kind of thing. But then the goal is to announce the alliance formally on May 14 at the Commerce Privacy Summit, and to make some concrete commitments to future activities in June.

"We support TRUSTe," notes Pearson. "We would also support a BBB-like model, hopeful that its brand name, combined with a well-designed privacy program (and whatever expertise they acquire to run one) would be successful as well." During the April 17 meeting, BBBOnline made its case to the group for funding. Our guess is that it won't be able to raise sufficient funds for the group (which would be unlikely to reach consensus on anything quite so concrete), but it benefited from the opportunity for a hearing and may indeed get some support directly from some of the organizations in attendance. One person there encouraged TRUSTe to come to Washington quickly to make a similar pitch.

What's good for IBM...

On the corporate front, IBM is hosting an invitation-only privacy conference for corporate customers in mid-May through its Institute for Advanced Commerce. Gerstner, who has a lot of different things to talk about, takes care to mention privacy at important moments, most notably last month at CeBIT. Indeed, IBM carries a lot of weight on this issue. Bigness is not always an advantage, but it does carry weight with governments and corporate customers worldwide. Correspondingly, IBM (like GM and Microsoft) is big enough that it cannot be healthy in a world where most people are sick. It desperately needs the Net overall and e-commerce in particular to flourish. In that way, it's like a government, concerned with the general welfare, and able (required?) to take something of a long view.

"The imposition of these deadlines is a good thing because it brings urgency... We come to the table with the sense that we're not leaving until this is done." - Harriet Pearson, IBM

NETSCAPE

Netscape plans to focus on complying directly with the EU data directive, says global public policy counsel Peter Harter. Of course, he acknowledges, it's not yet clear what that will require: "We're not sure our interpretation meets theirs." With some discussions for clarification, the company plans to meet that target by November. "We will also educate and encourage all our NetCenter partners to comply. In fact," he muses, "it could be a professional service we sell to our NetCenter partners - practical things like privacy auditing, posting a policy, getting a seal. These
are ongoing operational activities." As for industry coalitions, Harter, who previously worked in the public-interest world, says, "We'll support everybody. We've been behind TRUSTe for a while now, and we'll continue, but not exclusively. We are members of both TRUSTe and BBBOnline."

As noted, on the product side the company is also considering ideas such as privacy-policy detection in the browser. As a founding developer of the technology, it is also committed to supporting P3 in both browser and server products, but it hasn't yet committed to dates or details.

THE INTERACTIVE SERVICES ASSOCIATION

The Interactive Services Association is playing a leading role on the privacy issue, as part of an effort to coalesce the industry on privacy issues. Its recent response to the FTC's request for information illustrates the point that reality is better than it is sometimes painted: Its members all have privacy-disclosure statements of one kind or another. However, while all these companies post their policies, not all of them fulfill all of the ISA's suggested guidelines (see box). These companies provide services to almost 85 percent of US consumers with paid access to the Net or online services, or 23 million people, include America Online (including CompuServe), AT&T WorldNet, Bell Atlantic Internet Solutions, IBM Internet Connections Services, Internet MCI, Microsoft Network, Netcom, Pacific Bell Internet and Prodigy.

ISA has done a much other work on these issues, too. It has sent lots of information to the FTC; it also has an unusually well laid-out and informative Website. (Guess those membership dollars are being well used!) The draft notice and opt-out policy below (developed in conjunction with the Direct Marketing Association) is one example. Note that it does not say what should be done with the data, merely that the practices should be clearly disclosed - and give consumers a clear way to refuse the offer.

The ISA's privacy activism fits into a bigger picture. The 250-member ISA is one of several trade associations putatively representing the "Internet industry." Others include CIX, the Commercial Internet Exchange; ITAA, the former Adapso/American Data Processing Services Organization and the oldest of them all; the Interactive Industry Association (mostly for traditional online publishers); the Software Publishers Association, an upstart representing the pc software companies who felt ignored by the hoary Adapso membership and who are now in turn ignoring the Net community in favor of copyright protection for software publishers; and of course a variety of Internet organizations such as the Internet Society. But none of them adequately represents the vibrant, decentralized crew of Internet players whose livelihood depends on the success of this medium. (That's all of us, of course.)

So, meet the newly recast "Internet Alliance," about to be born out of the consumer-focused sections of the 15-year-old Interactive Services Association, perhaps just in time for the July "Global Framework" anniversary. The Alliance's raison d'être, says ISA chairman (and AOL director of law and global public policy) Bill Burrington, is "to grow the global online medium by building confidence and trust among consumers and policymakers."
A coherent message

After the industry's child-safety summit last December, Burrington notes, AOL's Steve Case and several other industry ceos considered the diffuseness of the so-called "Net industry." It may not need centralization, but a little coordination might help. After all, the White House considers this an industry, and so does the public. "Let's face it," says Burrington. "We're increasingly a prime-time industry; we need a prime-time Washington and Europe presence. So this year we decided to go out and raise several million dollars to build a first-rate proactive and effective Washington-based Internet industry association to build a real force in the consumer online market. We're focusing on consumers, not business to business."

The Interactive Services Association and Direct Marketing Association
Draft Online Notice and Opt-Out Principle

All marketers operating online sites, whether or not they collect personal information online from individuals, should make available their information practices to consumers in a prominent place. Marketers sharing personal information that is collected online should furnish individuals with an opportunity to prohibit the disclosure of such information for online solicitation purposes. This is a discussion document. We recognize that others also are examining these issues and we invite them to comment on our preliminary recommendations.

The Elements of the Notice

The notice should be easy to find, easy to read, and easy to understand. It should identify the marketer, disclose an e-mail and postal address at which it can be contacted, and state whether the marketer collects personal information online from individuals. If the marketer collects personal information online, the notice should contain disclosures about:

- The nature of personal information collected with respect to individual consumers.
- The nature of uses of such information.
- The nature and purpose of disclosures of such information, and the types of persons to whom disclosures may be made.
- The mechanism by which the individual may limit the disclosure of such information.

Means of Opting-Out

All marketers sharing personal information that is collected online should furnish consumers with the opportunity to request that their e-mail addresses not be rented, sold, or exchanged for online solicitation purposes, and should suppress in a timely fashion the e-mail addresses of individuals who have made such requests.
This is broader than privacy, Burrington notes, but privacy is the first, driving issue to get the process started. Time enough for Net taxation, commercial codes and the like. “The competition among associations; it’s just getting to be ridiculous,” says Burrington. “We need to bring in 15-20 key companies and trade associations at the ceo level: NRMA [National Retail Merchants Association], AAAA [American Association of Advertising Agencies], other third parties. It’s a three-bucket project: consumer education, accountability and recourse, and children’s marketing.”

“The problem with the kids’ safety summit was the aftercare. There was no continuing organization. There were a number of individual company efforts, but nothing coherent. We have to change that.”

- Bill Burrington, ISA and AOL

THE DIRECT MARKETING ASSOCIATION: RE-ENGINEERING A LEGACY ORGANIZATION

Until recently, the Direct Marketing Association seemed more concerned with avoiding trouble than taking the lead in privacy practices, but it is about to make its new “guidelines” [above] concerning data practices mandatory for its members. Robert Wientzen, president and ceo of the DMA, is leading his members into uncharted territory. They mail more than 80 percent of the direct mail in the US and make about 70 percent of the telemarketing phone calls (of which most are to existing customers, he hastens to note). Big question: Will some of them resign rather than follow the new rules?

For DMA members, the Net is still a peripheral concern...or so they think. Yet already more than 85 percent of members are on the Web (“making use of the Web for commercial purposes”), and 50 to 60 percent have commercial sites. Less than 2 percent send out unsolicited e-mails, although many are using e-mail for direct communications internally and with customers.

For years, the DMA’s privacy principles have sounded good, but they had no teeth. Ironically, the public’s concerns over privacy on the Net are starting to feed back into the much-larger (for now) offline marketing industry. “The Internet has brought questions to bear on traditional marketing, not the other way around,” says Wientzen. “Until two years ago, there were relatively few concerns about use of marketing data, although we’ve been at this privacy thing 30 years. It’s not a whole new ball game. Now, we’ve just spent $2.5 million on it.”

Making the guidelines mandatory, says Wientzen, “is a big issue. We’ve had no less than 500 hours of meetings in the last six months with a thousand people overall: When, how, who’s responsible, how to police it, and so on.” The new rules go into effect in July of 1999.

That may seem a long way away, but these companies are dealing with legacy systems, many of which need to be revamped to accommodate the kinds of data-tagging and processes the guidelines will require. The basic principles include regular disclosure of data practices, including a clear way for the consumer to opt out. “That’s called in-house suppression,” says Wientzen. “If people say they want out, they’re out. We honor it a minimum of five years (or 10 by phone).”

Separately, for lists maintained by third parties, the DMA already offers MPS and TPS (mail and telephone preference services). That’s for consumers
who want to say: “I don’t want to hear from anyone, even once...unless I get in touch with you first,” says Wientzen. “We have about 3.4 million names on the mail list, and 1.8 million on the phone part (because the number of households is lower than the number of individuals). Members of the DMA are encouraged to use that file before they phone or mail.” Currently, two thirds of them do. After all, reputable companies don’t want to waste money annoying people.

Next in line is EMPS, the Electronic Mail Preference Service. “We’re building it and will announce it in a couple of months,” says Wientzen. “We’re doing a contract with a major supplier to let individuals register and members can download it before mailing. We want to be make it easy for the little guys. We did have an pledge from [notorious spammer] Sanford Wallace to honor the EMPS before he folded his cards, but he’ll probably resurface.” In case you were wondering: No, the list will not be posted, and will in fact be highly secured. Would-be users, says Wientzen, will bounce their list against the DMA’s, which will offer the purging as a service. In other words, a would-be mailer has to have the address in the first place to have it removed...

This is a useful service, and should make a big change if the DMA can get it widely adopted; the problem is that the economics of mass e-mail are different from those of paper mail or telephone, allowing small, obscure e-mailers to cause a lot of trouble cheaply. And why should they join the DMA? As it happens, the DMA charges its members from $475 to $35,000 a year. It does not audit them regularly, but it does resolve disputes. “We’re hearing seven cases today,” Wientzen remarked on the day we talked to him. “We just threw out a fairly large company. No, it wasn’t an issue of privacy. They just weren’t being totally honest... That’s why mandatory is such a big deal.” (Of course, membership is voluntary.)

Moreover, the EMPS service misses the point of specific consumer choice; there’s no way to specify exactly which people you do and don’t want to hear from. It keeps you from hearing from anyone to whom you haven’t yourself e-mailed or somehow communicated. Nonetheless, EMPS sets a useful benchmark and provides a useful service. We hope the DMA makes it available free or at least cheaply. Long-run, we could imagine a combination digital ID and e-mail filtering service that would enable consumers (or their ISPs, as a service) to filter e-mail that did not have a DMA seal (and was not otherwise acceptable to the recipient).

DMA: Defining a Mission At-large

The DMA is also doing a good job of reaching out to other organizations. It developed the Notice and Opt-Out Principles (above, page 28) jointly with ISA, and co-sponsored a special publication for parents called “get cybersavvy,” full of realistic information about the dangers of cyberspace that end up being reassuring (because they have offline equivalents that we’ve all learned to live with). It also put up some of the funding for the World Wide Web Consortium’s work on P3P.

The DMA has also, as outreach to its own smaller members or total strangers, built a do-it-yourself privacy statement tool. “You answer a dozen questions and it will translate it into HTML and you can post it,” says Wiemtzen, the jargon tripping off his tongue. “Two thousand companies have adopted that thing. Now we’re getting 1600 or so visits a month. For small companies, it’s a godsend.”
“E-mail is going to be an incredible tool, and I want the big companies like IBM and P&G using it, because they'll do it responsibly, with target messages that are responsible and that people like receiving. Anything that interferes with trust has got to be stopped.”

— Robert Wientzen, DMA

FROM THE EDGE

We include this section warily, because we lack the space to do justice to all the arguments involved, but a few other groups deserve mention. Somewhat on the edge of this particular emerging market for privacy, a variety of groups are stirring the pot in their own ways. They include Europe, with which would prefer to negotiate with “the United States” rather than with all the organizations that make up its market; the Aspen Institute, which is asking whether a market for diverse privacy rules might emerge without extensive government “help;” and a variety of privacy advocates, who generally feel nothing but government regulation can overcome the power of large commercial interests, individual stalkers or other miscreants. Their voices are all being heard, but they are somewhat removed from the political/commercial negotiations described here. Call them “the environment” that surrounds the market.

Europe

The European Union comprises the largest body of Net users outside the United States, and therefore its actions matter greatly to the United States government and to the Net market - whatever that is. The overall European position on personal data favors much greater privacy, from press regulation to regulation of personal commercial data. (Ironically, European governments tend to collect far more data about their citizens, but they keep it private.) The fundamental “European” attitude is to be more trustful of government than we in the US are, and to see it as protecting rather than eroding the rights of citizens.

Moreover, to generalize, in Europe government is supposed to protect national culture and human values, whereas in the US we demand freedom and justice (and the courts) more than moral guidance from our government. This is reflected in the European position, which is to regulate the collection of personal data on a unified European basis, just as it regulates labor rights and many other issues. (Most notable, of course, is the forthcoming single European currency.)

The European Union has promulgated a "Directive" which goes into effect this October, and for which all EU members must implement complying legislation over the next few months (although observers expect it may take years to phase in). This directive requires strong protection for personal data, and restricts it from being exported to regimes where it is not so protected. The basic ideas are not much different from the Commerce Department’s Elements, but with a little more emphasis on regulation and less on choice. It is this directive that is driving European policy and putting pressure on the US government and US market players, because in principle the US as a whole could find it difficult to do business with EU citizens if EU does not find our protections satisfactory. On the other hand, “Europe” recognizes the need for strong encryption technology, although in Europe as in the United States the positions of law enforcement and of the
more commercially or human-oriented groups disagree. In short, none of these issues are fully resolved in Europe or the United States. It is unlikely trans-Atlantic commerce will stop with a bang come October, but finding some accommodation with the European position is important.

Privacy advocates

Privacy advocates, most notably the Electronic Privacy Information Center, likewise tend to think government regulation is the most suitable, effective means to protect citizens' personal privacy. They consider privacy a moral rather than a commercial issue, and they mistrust the self-regulatory efforts of commercial organizations. Moreover, they argue with some justification that the worst actors are unlikely to join the self-policing organizations that we describe above—unless they are forced to...most likely by government. These groups tend to focus on private-sector inadequacies rather than on how market forces might push them to become better—but of course we consider them part of the market that is indeed pushing towards better protection, even for the less aware.

Aspen Institute Technology Project: A broader context

The Aspen Institute, which has a tradition of exploring policy issues in the United States and the rest of the world, has now started a project to explore policy issues on the Net. Leading the effort is David Johnson, a legal scholar and founder of Counsel Connect, an online service for lawyers, and also former chairman of the Electronic Frontier Foundation. While the Europeans and the privacy advocates can be caricatured as requiring government involvement, he broadly questions the need for top-down government regulation of personal ("non-sensitive") data. Like the privacy advocates, he asks many of the right questions, even if there is little chance that he'll get the answers he seeks. (Indeed, that's what we consider the market of ideas.) Rather than focus on regulation or even self-regulation, says Johnson, "The government ought to assess the extent to which a private marketplace for privacy policies is emerging, whether 'customers' in that market are being given and making choices, whether the parties to the 'transactions' are satisfied, and so forth. We need a redefinition of the question away from 'Is the industry doing voluntarily what we would feel comfortable requiring them to do by regulation?' and towards 'Is there a robust and growing market satisfying the diverse consumer needs in this area?'

Furthermore, he notes: "The Commerce Department 'elements' don't give much scope or credit to innovative approaches using technology to shield information or to distribute marketing data back to users, or contracts that provide meaningful trust without the use of labels and auditing." He has asked whether something like a "Web-wrap" license might be used "upstream", by consumers to assert their rights, just as software publishers do with "shrink-wrap" licenses. Of course, this would require extremely well-informed consumers—or vendors or activists on the edge of the market who might help others to assert their rights. And it would move some issues from the legislature and administration to the courts. But it's an idea worth considering.
We are pleased to announce the arrival of Kevin Werbach as Release 1.0's new managing editor. Kevin comes to us from the Federal Communications Commission where he served as counsel for new technology policy. At the FCC, he was responsible for analyzing emerging communications technologies, and for developing policy on issues such as the treatment of Internet service providers, electronic commerce and broadband access. He is a recovering lawyer, whose current interests include Internet infrastructure, IP telephony, messaging, home-based networks, caching and streaming media. His work will begin appearing in next month's issues.

Jerry Michalski is moving on to independent consulting work but will continue to be a contributing editor to Release 1.0.
RESOURCES & PHONE NUMBERS

Bill Burrington, America Online, (202) 530-7880, fax 530-7879, billburr@aol.com
George Vradenburg, America Online, (703) 265-3999, fax 265-3995, vradenbur@aol.com
Casey Bennett, AICPA, (212) 596-6146, kbennett@aicpa.org, www.aicpa.org
David Johnson, Aspen Institute, (202) 736-3850, david.johnson@counsel.com or david.johnson@aspeninst.org
Russ Bodoff, BBBOnline, (703) 247-9331; fax, 243-5415, rboff@bbbonline.org
Ari Schwartz, Center for Democracy and Technology, (202) 637-9800, fax 637-0968, ari@cdt.org, www.cdt.org
Chris Barr, CNET, (415) 395-7800, chrisb@cnet.com, www.cnet.com
Becky Burr, US Department of Commerce, (202) 482-2581, bburr@ntia.doc.gov; www.ntia.doc.gov
Robert Wietsenz, Direct Marketing Association, (212) 768-7277, fax 768-7353, rwrientsen@thedma.org
Marc Rotenberg, David Sobel, Electronic Privacy Information Center, (202) 544-9240, fax (202) 547-5482, rotenberg@epic.org, info@epic.org, www.epic.org
Nick Grouf, Saul Klein, Firefly (Microsoft), (617) 528-1055, Nick_Grouf@firefly.net or NGrouf@microsoft.com, Saul_klein@firefly.net or SaulK@microsoft.com
Christine Varney, Hogan & Hartson, (202) 637-6823, cvarney@hlaw.com
Harriet Pearson, IBM, (202) 515-5036, hpearson@us.ibm.com
Roger Cochetti, IBM, (202) 515-5062, rcocchetti@vnet.ibm.com
David R. Yaun, IBM Research, (914) 945-3738,
Jeff Richards (also Bill Burrington of AOL, above), Information Services Association, (301) 495-4955, www.isa.net/policy/cons_awareness.html
Internet Content Coalition, www.netcontent.org
Bob Herbold, Edward Jung, Microsoft, (425) 882-8080, edwardj@microsoft.com, bherbold@microsoft.com
Jim Barksdale, Roberta Katz, Peter Harter, Sean Gaddis, Netscape, (650) 937-3024, jimb@netscape.com, roberta@netscape.com, pfh@netscape.com, seang@netscape.com, www.netscape.com
Martin Nisenholtz, NY Times Online, (212) 597-8092, fax 597-8081, martin@nytimes.com, www.nytimes.com
Shelly Lazarus, Ogilvy & Mather, (212) 237-6629
Ron Plessner, Piper Marbury, (202) 861-3969, rplessner@pipermar.com
Ira Magaziner, The White House, (202) 456-6406, magaziner_i@al.eop.gov
Susan Scott, TRUSTe, (650) 856-1525, fax 858-1936, sscott@truste.org, www.truste.org
Stratton Sclavos, Gregory Smirin, VeriSign, (650) 429-3462, stratton@verisign.com, gerg@verisign.com
Joe Reagle, World Wide Web Consortium, reagle@w3.org, www.w3.org/P3P

Release 1.0 23 April 1998
**Release 1.0 Calendar**

**1998**

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 4-8</td>
<td><strong>Computer Game Developers' Conference</strong> - Long Beach, CA.</td>
<td>Organized by Miller Freeman. The big annual game development event. Call (781) 821-6723; fax, (781) 828-9992; <a href="mailto:cgdc@mfi.com">cgdc@mfi.com</a>; <a href="http://www.cgdc.com">www.cgdc.com</a>.</td>
</tr>
<tr>
<td>May 10-11</td>
<td><em>Policy '98: Shaping Policy in the Information Age</em> - Washington, DC.</td>
<td>Organized by the ACM. Spans government, technology and education. Call (800) 342-6626 or (212) 626-0500; <a href="http://www.acm.org/usacm/events/policy98/">www.acm.org/usacm/events/policy98/</a>.</td>
</tr>
<tr>
<td>May 13-14</td>
<td><strong>Department of Commerce Privacy Summit</strong> - Washington, DC.</td>
<td>Meet just about everyone described in here and see their wares. Call Becky Burr, (202) 482-2581; <a href="mailto:burr@ntia.doc.gov">burr@ntia.doc.gov</a>; <a href="http://www.ntia.doc.gov">www.ntia.doc.gov</a>.</td>
</tr>
<tr>
<td>June 3-6</td>
<td><strong>International Design Conference in Aspen (the 48th annual)</strong> - Aspen, CO.</td>
<td>Organized by IDCA. The annual design conference, cutting across all design disciplines. Call (970) 925-2257; fax, (970) 925-8495; <a href="mailto:idca@csn.net">idca@csn.net</a>; <a href="http://www.idca.org">www.idca.org</a>.</td>
</tr>
<tr>
<td>June 8</td>
<td><strong>EPIC Cryptography and Privacy Conference</strong> - Washington, DC.</td>
<td>Sponsored by the Electronic Privacy Information Center, the Harvard Information Infrastructure Project and the London School of Economics. Conference agenda and registration information are available at <a href="http://www.epic.org/events/crypto98">www.epic.org/events/crypto98</a>.</td>
</tr>
<tr>
<td>Oct 11-13</td>
<td><strong>EDventure's High-Tech Forum</strong> - Copenhagen, Denmark.</td>
<td>Sponsored by EDventure Holdings. Call Daphne Kis, (212) 924-8800; fax, (212) 924-0240; <a href="mailto:daphne@edventure.com">daphne@edventure.com</a>; <a href="http://www.edventure.com">www.edventure.com</a>.</td>
</tr>
</tbody>
</table>

* Events Esther plans to attend.  
@ Events Jerry plans to attend.  
Lack of a symbol is no indication of lack of merit.  
The full, current calendar is available on our Website (www.edventure.com).  
Please let us know about other events we should include. — Mari Katsunuma
SUBSCRIPTION FORM

Please enter my subscription to Release 1.0 at the rate of $795 per year in the U.S. and Canada. Overseas subscriptions are $850, 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 ☐ Master Card ☐ Visa
  Card Number ___________________________ Expiration Date ________
  Name and Billing Address ______________________________
  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