APPENDIX E:

Advisory Group Comments

Table of Contents

American Express Company
Statement on the Georgetown Internet Privacy Policy Survey

The results of the Georgetown Internet Privacy Survey provide visible evidence that the business community has made significant progress over the past year in understanding the importance of providing consumers with information about what personally identifiable information is collected on Web sites and the choices they have in controlling the use of their information.

Self Regulation – An American Express Example

American Express has supported industry self-regulation of privacy for more than 25 years by demonstrating its commitment through action.

- In 1974, we were the first in our industry to offer consumers the option of being excluded from mailing lists used for marketing offers ("opt-out").
- In 1978, we began issuing to employees a Privacy Code of Conduct.
- In 1991, we adopted and publicly distributed the American Express Customer Privacy Principles.

- Briefings were held with senior management and a comprehensive Privacy Resource Kit was provided to managers and trainers at all American Express units around the world. In addition, the Principles were published in seven languages to facilitate communicating with a global multi-lingual employee base.
- A number of leading privacy experts have reviewed our Privacy Principles and materials to help ensure that we are at the forefront of protecting consumers.
- The Principles define the company's commitment to protect the privacy of its customers. Each business unit maintains its own additional rules and practices which are fully consistent with these Principles, and which they may modify as needed for particular products and services, or to conform to local laws or customs around the world.

We have adapted our policies to recognize technological advancements like the Internet.

- In 1997, we updated our Customer Privacy Principles to include our online business initiatives.
- In February 1998, we posted a Customer Internet Privacy Statement on our corporate Web site at www.americanexpress.com. This statement – which is based on our Customer Privacy Principles and is easily accessible on every page of the Web site –provides a full description of Web site security, information collection and use, how to decline email offers, and a statement about our commitment to privacy protection.
- Also in February 1998, we provided customers with the ability to decline receiving email offers online ("opt-out"). Customers can use the "Set Email Preference" page to change their choices.
- In addition, every email offer provides a privacy disclosure and an easy reply mechanism to opt-out of future marketing email offers.

Security

We have also built online safeguards to ensure that all customer information remains secure. When customers send or receive confidential personal account data through the American Express Web site, we require that a "secure session" first be established using the Secure Socket (SSL). SSL enhances the safety and confidentiality of transmissions of private information on our Web site over the Internet.

Consumer Education

American Express has been active in providing consumer education about privacy beginning in 1992 with the development of a brochure, "Protecting Your Privacy." Several hundred thousand copies of the brochure were distributed with the help of the US Consumer Information Center. It was made available on the Center's Web site, and remains available on American Express' Web site. Later, American Express produced an educational resource kit for high school and college teachers. More than 20,000 copies have been distributed. The kit – titled "Who Knows? Your Privacy in the Age of Information" – contains a resource guide and a poster, as well as discussion and student-activity materials. The Canadian government adapted the kit to correspond to Canadian laws and made it available to all schools across Canada via the school's Intranet.

In 1996, American Express produced the brochure, "Cybershopping – Protecting Yourself When Buying Online," with the co-sponsorship of the Consumer Information Center and information assistance from the Federal Trade Commission. A revision, "CyberSmarts," was published in 1998 and added as co-sponsors, Call for Action and The Direct Marketing Association. American Express participated in developing Call for Action's ABC's of Privacy and helped to fund posting them on Call For Action's Web site.

In 1999, we published "Shopping Safely Online" – a further revision of the CyberSmarts brochure with the same co-sponsors.

Enforcement

In 1998, American Express helped to fund the development of the BBBOnline Privacy Program and was an active participant in developing the self-assessment tool and dispute resolution process. This voluntary program provides a framework for companies to self assess the adequacy of their privacy policies and whether they have been fully implemented. An extensive tutorial built into the self-assessment provides background for companies who may be taking the first steps in developing a privacy policy and implementing it.

Center for Democracy and Technology
Comments on the Georgetown Internet Privacy Policy Survey

The Center for Democracy and Technology (CDT) is pleased to have this opportunity to comment upon the Georgetown Internet Privacy Policy Survey. CDT is committed to realizing civil liberties on the Internet consistent with the decentralized, global nature of this new medium. Because of the nature of the World Wide Web, implementing privacy protections on the global and decentralized Internet is a complex task that will require new thinking and innovative approaches.

Because many Web sites will need some baseline policy guidance and self-enforcement may not always be a viable remedy, we believe that legislation, as well as robust self-regulation will be both inevitable and necessary to make consumer privacy on the Internet the rule rather than the exception.

That a combination of means---self-regulation, technology, and legislation---are required is established by the most recent Georgetown Internet Privacy Policy Survey. As we analyze below, the study shows that definite progress has been made in making many more Web sites privacy sensitive. But those numbers also show that real fair information practices are incorporated by only a small number of sites and most sites have yet to embody more than minimum disclosure of their information practices.

To achieve real privacy on the Internet, we will need more than better numbers, redoubled efforts by industry, or a legislative mantra. We will need a good-faith concerted effort by industry, consumer and privacy advocates, and policymakers to develop real and substantive answers to a number of difficult policy issues involving the scope of identifiable information, the workings of consent and access mechanisms, and the structure of effective remedies that protect privacy without adversely affecting the openness and vitality of the Internet.

As the Federal Trade Commission's rulemaking under the Children's Online Privacy Protection Act and industry's various efforts at self-regulation attest to, these issues are not easy. But armed with the findings of the Georgetown Internet Privacy Policy Survey, we believe interested parties are in a position to move forward on a three pronged approach – expanded self-regulation, work to develop and deploy privacy-enhancing technologies such as P3P, and legislation -- all require a serious dialogue on policy and practice options for resolving difficult issues in this promising medium.

The Facts

CDT strongly believes that good policy is based upon a solid understanding of the facts. The Survey supplies factual information on the quantity of privacy notices on the World Wide Web. When combined with information about the quality and effectiveness of Web sites' privacy practices and the reach and effectiveness of oversight and enforcement mechanisms,[1] the Survey can provide the basis for developing sound national policy on online privacy. While the Survey reveals some progress, it demonstrates that we are far from achieving our shared goal of "broad-based and effective [privacy protections]."[2]

The Survey findings reveal modest steps forward in some areas, but substantive privacy protections are still far from ubiquitous on the World Wide Web. On the positive side, the Survey reveals **a** growing privacy consciousness -- perhaps spurred by survey upon survey documenting consumer concern and anxiety -- among companies operating online. This is evidenced by an increase in the number of Web sites that are providing consumers with some information about what personal information is collected (44%), and how that information will be used (52%). Companies that are posting fuller information about their data handling[3] are more likely to have a link to such statements from the home page (79.7%) than they were a year ago.[4]

However, on important issues such as access to personal information and the ability to correct inaccurate information, only 22% and 18% respectively of these highly trafficked Web sites provide consumers with notice. On the important issue of providing individuals with the capacity to control the use and disclosure of personal information, the survey finds that 39.5% of these busy Web sites say that consumers can make some decision about whether they are re-contacted for marketing purposes -- most likely an "opt-out" -- and fewer still, 25%, say they provide consumers with some control over the disclosure of data to third parties.[5]

---

[1] CDT will be providing a separate report to the Commission assessing the quality of practices on the Web and examining the Self-regulatory seal programs.

[2] PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION ON "CONSUMER PRIVACY ON THE WORLD WIDE WEB" Before the SUBCOMMITTEE ON TELECOMMUNICATIONS, TRADE AND CONSUMER PROTECTION of the HOUSE COMMITTEE ON COMMERCE UNITED STATES HOUSE OF REPRESENTATIVES Washington, D.C. July 21, 1998.

[3] The report calls these "privacy policies" as compared to "information practice statements." "Privacy policies" are a more comprehensive description of a site's practices that are located in a single place and accessible through an icon or hyperlink. A site may have a "privacy policy" by this definition but still not have a privacy policy that meets the elements set out by the FTC or various industry self-regulatory initiatives for an adequate privacy policy.

[4] In response to the question, "Is a Privacy Policy Notice easy to find?" surfers in the 1998 survey answered yes for approximately 1.2% of Web sites. FTC Report, Appendix C Q19.

[5] This number is generated using the data from Q32 (number of sites that say they give consumers choice about having collected information disclosed to outside third parties) -- 64 -- and dividing it by 256 (the total survey sample (364) minus the number of sites that affirmatively state they do not disclose data to third-parties (Q29A) (69) and the number of sites that affirmatively state that data is only disclosed in the aggregate (Q30) (39)).

Robust privacy notices are the exception not the norm. The Survey reveals that at over 90% of the most frequently trafficked Web sites[6] consumers are not being adequately informed about how their personal information is handled.[7] At the same time the survey found that over 90% of these same busy consumer-oriented Web sites are collecting personal information.[8] In fact, the survey revealed an increase in the number of Web sites collecting sensitive information such as credit card numbers (up 20%), names (up 13.3%), and even Social Security Numbers (up 1.7%).

Thus, while many companies appear to be making an effort to address some privacy concerns, the results from the consumer perspective appear to be a quilt of complex and inconsistent statements. While progress is evident in some areas the number of sites that provide consumers with the types of notices required by the Online Privacy Alliance, the Better Business Bureau and TrustE is still relatively small (9.5%).

Towards meaningful privacy protections on the World Wide Web

Like the FTC, the Administration, and industry, we are heartened by the increased attention to various elements of the Code of Fair information practices evidenced by the survey results. We have welcomed efforts by the Commission and others to drive best practices in the marketplace. We are not wedded to a particular method or enforcement scheme, but rather seek effective and robust privacy protections for consumers in the growing area of electronic commerce.

In its Testimony last July, the Commission stated that, "…unless industry can demonstrate that it has developed and implemented broad-based and effective self-regulatory programs by the end of this year, additional governmental authority in this area would be appropriate and necessary."[9] Despite the considerable effort of the Commission, the Administration and industry to encourage and facilitate an effective self-regulatory system to protect consumer privacy, based on the survey results we do not believe that one has yet emerged.

Last year, the Commission offered a legislative outline that embodied a framework, similar to the one we suggest, building upon the strengths of both the self-regulatory and regulatory processes. As the Commission moves forward this year, we look forward to working with you and all interested parties to ensure that Fair information practices are incorporated into business practices on the World Wide Web. Both legislation and self-regulation are only as good as the substantive policies they embody. As we said at the start, this requires resolving several critical issues. Here is

[6] Only 9.5% of the most frequently visited Web sites and 14.7% of those that collect information had privacy policies containing critical information called for by the FTC, the Administration, and required by the Online Privacy Alliance, TrutstE and the BBB Online, about notice; choice; access; security; and contact information.
[7] Last years survey found approximately 2% or Web sites that collected data, and less than 1% of all Web sites, had adequate notices.
[8] 92.9% are collecting some type of personal information.

a partial list of issues to be resolved: When is data personally identifiable? The Pentium III PSN and the rulemaking under COPPA have brought this issue before the Commission. Similarly, the question of structuring a consent model and appropriate rules for access to information loom large in this complex environment. Finally, regardless of where remedies are meted out, we must collectively wrestle with how to best ensure compliance, measure damages, and encourage compliance. Regardless of whether you believe in self-regulation, legislation, or some combination thereof, we think all parties should engage in a good-faith effort to answer these questions. With a three-pronged effort – self-regulation, technology, and legislation -- we believe that real privacy protections that map onto the Internet are within reach.

* * * * *

CDT is a non-profit, public interest organization dedicated to developing and implementing public policies to protect and advance civil liberties and democratic values on the Internet. One of our core goals is to enhance privacy protections for individuals in the development and use of new communications technologies.

[9] Last years survey found approximately 2% or Web sites that collected data, and less than 1% of all Web sites, had adequate notices. Privacy Online: A Report to Congress, Federal Trade Commission, June 1998.

Consumer Federation of America & Consumer Action
Statement on the Georgetown Internet Privacy Policy Survey

One last chance.

The FTC told the House Commerce Subcommittee on Telecommunications, Trade and Consumer Protection last year: "Unless industry can demonstrate that it has developed and implemented broad-based and effective self-regulatory programs by the end of the year, additional governmental authority would be appropriate and necessary."

In January of this year, FTC Chairman Robert Pitofsky stated: "We want the industry to self-regulate. But it is possible we would consider proposing legislation later this year, if it is clear that self-regulation by the industry is not working."[1] The decision on whether to recommend legislation was said to depend on the results of a new "sweep", or survey, of commercial World Wide Web sites to be conducted by a private consortium headed by Professor Mary Culnan.

Industry had fair warning and ample opportunity to adopt and enforce voluntary privacy policies and fair information practices ahead of the 1999 "sweep." The FTC announced its intention to monitor progress with self-regulation in 1998.[2] The Online Privacy Alliance, Better Business Bureau and TRUSTe announced a campaign to encourage thousands of technology companies and Web site owners to adopt privacy policies as a "last-ditch effort to avoid new laws that could stunt the growth of e-commerce" in advance of the 1999 survey.[3] The Direct Marketing Association reminded its members in February to make sure their online privacy policies are in order before the FTC sweep of sites' data protection policies.[4]

The results are in.

Fewer than 10% of the sample Web sites meet the minimal fair information practices standards supported by the FTC, professed by industry self-regulation proponents, and expected by consumers. Industry self-regulation fails to protect consumers or foster consumer confidence in electronic commerce. Further failure by Congress and the FTC to enact comprehensive privacy protections will handicap the development of electronic commerce.

The report documents the almost universal practice of collecting personal identifying information (92.9% of Web sites collect personal identifying information.) Over half the sites (56.9%) collect demographic information. The average site that collected personal identification collected an average of 3.66 elements of personal information in addition to name or e-mail address.

[1] "FTC, Key Members Eyeing Internet Privacy Safeguards," CQ Daily Monitor, January 27, 1999, p. 1.
[2] "Privacy Online: A Report to Congress," Federal Trade Commission, June 1998, p. 42-43.
[3] Maria Seminerio, "FTC privacy study looms," ZDNet, March 1, 1999.
[4] Robert MacMillan, "DMA Urges Sites To Pull Up Privacy Pants," Newsbytes, February 3, 1999.

The survey found that 65.7% of sites in the sample posted privacy notices that contained at least one privacy disclosure and 70% of the Web sites that collected personal information posted at least one type of privacy disclosure. However, only 14.8% of the same 237 Web sites contained the bare minimum on at least one survey element for notice, choice, access, security and contact information.

Despite this low compliance figure, the 1999 results, graded on a pass-fail basis, are being portrayed by the industry as a sign of great progress. When actual performance according to the FTC's fair information practices standards is graded, the industry fails. Meaningful and effective privacy protections for consumers are largely missing.

Consumers who use the Web to browse, access information, or make purchases place a high importance on protection of their personal information. A 1998 opinion poll conducted by Business Week and Louis Harris & Associates found that 78% of persons who use the Internet said they would increase their use of the Internet if they believed their privacy were protected. A majority said that if a company explicitly guaranteed the security of personal information, they would be encouraged to register on the Web site, provide personal information, and purchase products or services. Two-thirds said that if a company posted its privacy policy, they would trust the company to follow that policy.

Consumers also support legislation to protect their privacy online. Fifty-three percent said the government should pass laws now governing how information can be collected and used on the Internet.[5] As Business Week noted in an Editorial March 16, 1998, "Time is running out for the Net community. The public does not trust its promises for self-regulation to ensure privacy. The polls show that people don't believe that these voluntary standards are working. Any spot check of Web sites shows that few make any serious effort to protect privacy. It's no wonder that the public wants the government to step in immediately and pass laws on how personal information can be collected and used... Future growth depends on the security of that data and the comfort level for that behavior. Both civil society and economic growth depend increasingly on privacy."[6]

[5] Jennifer Kingson Bloom, "FTC to audit banks' Web-site privacy policies," American Banker, March 6, 1998, at 1, 12.
[6] Editorial, "Privacy: The Key to the New Economy," Business Week, March 16, 1998, p. 126.

The Direct Marketing Association
Statement on the Georgetown Internet Privacy Policy Survey

The DMA (The DMA) believes the study shows that business has heeded the call from The White House and the Federal Trade Commission (FTC) to promote privacy protection online through the adoption of self-regulatory measures.

For the last two years, The DMA has worked to help business sites understand the importance of posting a privacy policy. To make this easy we developed a privacy policy tool, which is posted on The DMA Web Site (www.the-dma.org), and we have encouraged any organization to use it: we know that hundreds of interactive marketers have used this resource.

We are happy to see that the collective efforts of The DMA, the Online Privacy Alliance, the Council of Better Business Bureaus, Trust-e and others have made a major difference both in helping business to understand both the importance of posting privacy policies, and in actually posting them effectively.

The study found that two-out-of-three of the top 7500 ".com sites" visited by consumers carried a privacy policy. (The unduplicated reach of the sampling frame is 98.8% of total U.S. Web traffic.) This progress, while not directly comparable to last year's survey (where approximately one-in-seven posted a policy) is nevertheless quite significant.

The study also found that 87% of the sites with a privacy policy included a notice element and 77% included a choice element. Lower percentages (49%, 46% and 40%, respectively) contained a statement about contact information, security and access. This is not surprising, as consumers assign much different concerns about security and access depending on the nature of the information at hand.

The DMA's efforts have been focused on notice and choice as we continue to read the marketplace as to what are the most important elements of a privacy policy from a consumer perspective. Contact information is not so important to consumers who already know how to find your Web site and communicate with you. While security is important about sensitive data, much of the data transferred between Web site and consumer is not sensitive and doesn't raise these issues. As far as access is concerned, it is not common that a consumer would contact a company that they do business with and ask randomly for all information it ever collected about them. As the representative of almost 5,000 companies involved with marketing data, we can testify that such a request is not typical.

Consumers may have a specific billing questions (already addressed under the Fair Credit Billing Act). Or they may want to know where their name was sourced (and our guidelines state that the source should be revealed upon request of a consumer). But access to all data would present a burdensome, complicated, expensive and unusual request. Most importantly, consumers are not demanding this information among businesses and non-profit groups in this economic sector.

The DMA will continue to promote the posting of privacy policies over the next year. We do this, because it is the right thing and because we believe that it will continue to build consumer trust.

Consumers are showing a great level of comfort as e-commerce booms: on-line sales approached $6 billion in 1998, and sales are expected to exceed $11 billion this year. The DMA continues to forecast growth in e-commerce direct marketing sales above 60% per year through 2003—assuming continued consumer confidence and lack of new regulatory requirements.

According to The DMA's second Web Site Evaluation Study, 76% of Web users surveyed indicated that they ordered something online in the last six months and 73% had bought something from a mail order catalog.
To continue to build consumer confidence and help the FTC and the White House, The DMA will revise its privacy policy tool to make it more directly applicable to a broader view of a comprehensive privacy policy. We will also broaden our reach to more and smaller businesses, working directly through DMA networks, and in a leadership position as part of the Online Privacy Alliance.

Indeed our “Privacy Promise” initiative provides us a strong platform from which to be effective. As of July, all DMA members that exchange consumer data, as a condition of membership, must provide consumers with notice and opt-out options regarding their use of consumer information for marketing purposes.

We appreciate the opportunity to comment and look forward to continuing our work in this area.

Patricia Faley
Vice President
Ethics and Consumer Affairs

IBM Corporation
Comments on the Georgetown Internet Privacy Policy Survey

On behalf of IBM Corporation, I would like to commend and thank Professor Mary Culnan and all of those who have worked with her for the significant contribution that they have made to the public's understanding of contemporary privacy practices on the Internet's World Wide Web through this study. I particular, we express our appreciation to Georgetown University, Ernst and Young, Media Metrix, and the fifteen students who worked with Professor Culnan in making this study possible.

The study reveals a lot that is important to anyone interested in both the evolution of the Web and how governments anywhere should react to that evolution, particularly when its results are compared with the results of a similar study conducted by the Federal Trade Commission about a year earlier. While these two studies are not exactly comparable, the differences in their basic results point to a dramatic shift in commercial practices on the Web in the space of about a year: Whereas in 1998, around one out of six of the commercial Websites most frequently visited by Americans disclosed something to their Website visitors about what personal information was being collected and how it would be used, by 1999 that proportion has risen to around four out of six.

This very significant improvement should neither be under nor over stated. It demonstrates without question, in our view, that today, normal commercial conduct on the Web for Americans is that they are provided some key information about how their personal information is collected and used. For people not familiar with the on-line medium, it is often hard to believe that in the space of one year, on-line privacy protections could have gone from a position of being significantly below consumers' experience in the off-line world to a position of being significantly better than their experiences in the off-line world. But the reality is that this medium can, and does, turn around just that quickly.

We doubt that the turn-around that we have seen since last year can be described as success. Not only does the study reveal that two of six of the commercial Websites most frequently visited by Americans provide no information about what personal information is collected and how it is used, but it also reveals that the spread of disclosure of privacy practices is broader than it is deep. This leaves much to be done; not only in moving the remaining commercial Website operators who fail to disclose their practices, but also in reaching out to those operators who currently are making minimal disclosures and seeing that they strengthen their practices. IBM, along with many other companies and with Internet privacy organizations that we support like the On-Line Privacy Alliance, the Better Business Bureau On-Line and TRUSTe, is committed to that

effort. We are convinced that the conditions on the Web a year from today will show as dramatic an improvement over today's practices as the improvement that we have already seen from 1998 to 1999.

The reason we are convinced that commercial Website privacy practices will continue to improve is that it is good business for each and every commercial Website operator to do so, and the vast majority of commercial Website operators are businesswomen and businessmen who are investing in electronic commerce for the long haul. They understand quickly that their most important relationship in a medium like the Web is the relationship of trust that they have with each customer, and that this relationship is driven, as much as anything else, by the extent to which the customer feels the commercial Website operator respects the customer's interests in privacy. In the medium of the Web, merchants who demonstrate little or no such respect will find themselves being abandoned by their customers, while those who demonstrate such respect for their customers will find that doing so has strengthened their customers' loyalty. We have found that commercial Website operators understand this dynamic and have rapidly changed their practices to strengthen consumer trust in their Websites; in part because many such operators are small businessmen and women, who are themselves both consumers and enthusiastic Web surfers.

Roger J. Cochetti
Program Director - Policy & Business Planning
IBM Corporation

Ram Avrahami / The NAMED
Comments on the Georgetown Internet privacy Policy Survey

Executive Summary

The Georgetown University-conducted survey of the top 7,500 visited commercial sites, which was requested by the FTC and funded by industry, looked at the easier to measure aspects of privacy and found some troubling realities underneath the surface. While the number of sites who post privacy policies has probably been increasing, privacy practices are still far from minimum standards and default privacy among large sites was found to be worse than on smaller ones.

An analysis of issues in the sampling and measurement methodology as well as the results of the survey reveals several points that should be taken into account in understanding the results of this survey as well as the planning of future ones. The change in sampling methodology made it impossible to properly compare last year's sample of 226,600 sites with this year's 7,500. The inclusion of portals in the sample presented a misleadingly high rate of 98.8% consumer traffic, because it includes the portal-only traffic as well. The efforts of industry groups to prepare sites for the survey also biased the results in an uncertain way. As objective and accurate measurement of Fair Information Practices (FIPs) is difficult, it is important to understand what was actually measured in this survey and design ways to improve it in the future.

Despite the difficulties in measurement and some misinformation in the interpretation by the media, the survey results revealed several troubling realities about the status of Internet privacy. Less than 10% of sites have all 5 elements of the FIPs measured by the survey, and comparison between the top 7,500 sites and the smaller group of top 100 sites shows unexpectedly that the default privacy practices in the top 100 sites are worse than in the other group. It appears that, the more sophisticated the sites are, the more information and choices they provide to consumers but also the more likely they are to use consumer information without permission.

The text below discusses these issues in more detail and provides some suggestions to improvements in future surveys.

Background

Professor Mary Culnan of Georgetown University conducted a survey in March 1999 of the 7,500 most visited commercial web sites (the sites were selected by Media Metrix, an Internet monitoring and measurement company). The survey has been identified by different names, but in these comments it will be referred to as the Culnan Survey or simply the Survey. The Survey was supposed to be a follow up to last year's survey conducted by the FTC, and the FTC provided compatibility requirements which delineated the bulk of the survey structure. An advisory committee, consisting largely of industry personnel and a minority of consumer and privacy advocates, provided input, via several meetings and some online discussions, to Prof. Culnan, but all Survey decisions were taken by Professor Culnan alone. Industry members on the committee provided the funds for the survey.

Sample Methodology: Comparing Frames of 100/111 vs 7,500 vs 226,600

Last year the FTC surveyed 6 “frames” of sites - 3 sectorial (finance, health, retail), one children, one of the top 111 and one of ‘all’ (226,600) commercial dot.com sites. This year the FTC decided that it need not check the sectors separately (all sectors had similar results last year) nor the children sites, and discussions were held on which frame to sample - top 111, all (226,600) or somewhere in between. Because of budget constraints, the advisory committee was notified that it was possible to survey 300 sites only, which prevented the sampling of all three frames with reasonable statistical validity. Industry objected to the option of all (226,600) sites as including many sites which do not have serious consumer traffic, while

privacy advocates opposed the top 100 option as including only few and predetermined sites that would not be representative of the rest of Internet sites. A compromise was reached to take a sample from a frame of enough sites to cover 99% of sites, which eventually constituted the sampling of 364 sites from the top 7,500. (see also discussion on portal regarding the validity of the 99% figure)

Having decided on the compromise, the OPA contracted Mary Culnan to conduct a parallel survey of the top 100 sites, which is roughly compared to the top 111 from last year. This survey will be referred to as the OPA Survey. The frame of all (226,600) commercial sites was not measured this year.

Although clearly understood and stated by members of the advisory committee from all sides, as well as clearly delineated by the Survey report (Section IIA and Table 1), there seemed to have been confusion in the media regarding the ability to compare between the 1998 FTC survey results and the 1999 Culnan Survey results. It is impossible to know if measuring “65% penetration of the top 7,500 sites in 1999” compared to “14% penetration of top 226,600 sites in 1998” shows any progress or not. It is conceivable that the top 226,600 sites would still have shown only 14% penetration if measured in 1999, meaning that absolutely no progress was made since last year. Even if there was progress, there is no way to know how much it was without a measurement. Similar reasoning applies to any progress in the frame of 7,500 sites, as they were not measured in 1998.

Sample methodology: Portals

One of the issues debated early in the advisory committee was whether to include portals in the sample. Since portals are often used only as a transitory path to the actual destination of the consumer, it is not clear whether such use should be counted as a "consumer visit". To make matters complicated, many portals have developed content areas to attract transitory consumers to stay in the site. Hence, portals sites could not be simply excluded.

In the end, portal sites were fully included in the samples, which likely biased the traffic figures upwards. Together with portals, the top 100 sites were stated to cover 94.4% of web traffic, while the next 7,400 cover merely 4.4% more. Without portal traffic, the top 100 coverage may be significantly lower (perhaps down from 94.4% to 70%) while the top 7,500 coverage is probably closer to its current level (perhaps down from 98.8% to 90%). It may be possible to conduct a more accurate analysis if Media Metrix does a finer analysis of the traffic behavior of their recruited surfers on portal sites to distinguish between the portal function and the content parts of the sites.

Sample Methodology: Threshold

The threshold used for this survey - top 7,500 - was taken somewhat arbitrarily. The idea was to get as much web traffic as possible and 7,500 was a round number that got close to what Media Matrix could deliver. As it turns out, this threshold represented three separate numerical thresholds:
1) Top 7,500 visited sites
2) Top sites covering 98.8% of visits
3) Sites having 32,000 visits a month or more (32k+v/m)

While this year all three thresholds merged, it is clear that this will not be the case in future years when the Internet grows. Hence, it may be important to understand the conceptual difference between these thresholds for future comparisons.

The Top 7,500 threshold is a round number, but will capture less traffic as the web grows. Thus, it will not be a good measurement for overall web traffic in the long run. Both the top 98.8% and 32k+v/m thresholds will accommodate more sites as the net grows, but they will differ based on the pattern of growth. 32k+v/m is an absolute threshold and is easy to measure and determine for each site if included within the frame or not. However, if there will be much growth in very small sites, then the frame of 32k+v/m sites may lose a significant portion of the consumer traffic. The 98.8% threashold will always be the best threshold for

capturing a fixed portion of consumer traffic, but may become harder to compare to other measurements besides itself.

Measurement Methodology: What Are Fair Information Principles (FIPs)

There is a confusion as to what constitutes Fair Information Practices (FIPs). The FTC stated in its 6/98 Report to Congress that a series of studies and guidelines issued by US and other OECD governments in the past quarter of the century define various principles that should govern fair handling of personal information.

Without a canonical set of principles, it may have been advisable to monitor market behavior on a complete set of all these principles. However, the FTC decided to focus on an intersection set of 10 principles which it stated are common to most of these studies (the principles are grouped in couples but each is distinct in meaning):

1) Notice/Awareness
2) Choice/Consent
3) Access/Participation
4) Integrity/Security
5) Enforcement/Redress

(http://www.ftc.gov/reports/privacy3/fairinfo.htm#Fair Information Practice Principles)

The Survey reduced this set further to 5 principles - Notice, Choice, Access, Security and Contact (part of Redress). Section IIIC of the Survey report describes how these 5 principles are defined for the purpose of the Survey. Appropriately, the Survey calls these five - "elements of FIPs", as it does not assume that it covers full principles but only parts of it.

Measurement Methodology: "Easy Grading"

Following last year's FTC methodology, this year's survey also used "easy grading". Policy statements by sites were used to their credit as much as possible. Often, the mention of a subject resulted in a full credit for that subject.

For example, a site that merely says “click here if you do not want to be on our mailing list” or “It is safe to transmit your credit card number using our secure server” or even “If you have questions about our privacy practices, send us an email” received full credit for Notice, as posting an Information Practice Statement (app. D, pp6). If the Survey had required an actual privacy policy to get full credit, the percentage of sites that complied with the Notice element would drop from 66% to 43%. Requiring complete disclosure would have reduced the percentage further.

Similarly, "easy grading" applied in analyzing the notice content. Questions Q23-Q26, Q31, Q35 and Q36 start with “Does the site say anything about…”, so any mention of one out of potentially many practices got full credit. Similar implications can be inferred for questions Q28, Q29, Q32, Q33, Q34, Q37 and Q38, which gave credit to a mention of practice without qualification to the scope of such practice.

Measurement Methodology: Direct measurement of Fair Information Principles

The Culnan Survey measured directly only one FIP - Notice. Other elements of FIPs were inferred from statements in the Notice regarding specific practices used by the site. However, even if the sites are truthful in their statements, it is difficult or sometimes impossible for an outside observer to tell whether a site discloses all of its practices or only a portion of them. Thus, it is imperative that the sites themselves state that they do not have any additional undisclosed practices and that surveys measure such 'completeness' statements. The current Survey had only one such example - question Q30 - “Does the site say that it only discloses this information to outside parties in aggregate form?” (underline in the original)

The following ideas may be helpful to measure FIPs directly, without relying on Notice statements:

- Sites can answer a questionnaire, stating exactly which FIPs they adhere to.

- Trained surfers can check whether the personal information collected is relevant to the direct purpose for which it was collected (Collection Limitation Principle - OECD guidelines) and if the purpose of use is specified at the time of collection (Purpose Specification Principle - OECD guidelines).

- Sites can count how many people actually visit their policies web pages and consumers can answer a questionnaire, stating how aware they are of the details of the policies. (Awareness - FTC Guidelines).

Results: Bias Due To Pre-Survey Industry Warning Efforts

The media reported that in the month before the survey took place, the DMA, OPA, BBBonline and TRUSTe put in an effort, which included sending out thousands of letters, warning businesses about the upcoming survey and requesting them to prepare for it. “The Online Privacy Alliance, the BBBOnLine, and TRUSTe today announced a joint outreach campaign to encourage commercial web sites to post privacy policies before the start of a Web survey March 8.” stated a joint release on March 1, 1999. This effort probably was directed to, and could have made a significant impact on, the 7,500 sites which the Survey sampled.

An example to the content of such warning was available on the DMA site. An animated image (http://www.the-dma.org/home-menu/images/dma_ftc_anim.gif), warned businesses on the upcoming survey and led them to a web-alert page which stated the following:

> “In June, The Federal Trade Commission reported to Congress on the status of privacy on the Web. An FTC scan of the Web found that only 14% of commercial sites had privacy policy statements. Based on these results, the FTC recommended that Congress create legislation to ensure consumer privacy on the Web. In January, the FTC is expected to make a second recommendation based on industry progress since the June report and, if progress is not made in the area of online notice, the FTC will appeal to Congress for government intervention on the Internet. Any regulation of the Internet could stifle the growth of this exciting new marketing medium, restrict the use of information gathered online, and set a precedent for regulation in other media.
>
> To help The DMA show that self-regulation is effectively addressing consumer privacy needs, it is critical that your company post a Privacy Policy Statement on its Web site!
>
> The DMA has created the tools you need. We have developed a Privacy Policy Generator that will allow you to create and post a Privacy Policy Statement to your Web site in a matter of minutes. The Generator gives marketers an "add water and stir" recipe for providing consumers with information on how data is gathered and used online.
>
> In addition, The DMA's Marketing Online: Privacy Principles and Guidance provides marketers with information about disclosure of online information practices. Please take a moment to review these resources and use them to develop an Online

Privacy Policy for your site.

So post your Privacy Statement today."
(taken from http://www.the-dma.org/home/web-alert.html 5/24/99)

While an educational effort to promote privacy is generally welcomed, the timing and reasoning of this effort raises concern that it resulted in a speedy ad-hoc posting of privacy policies (which is relatively easy to do) but not the long term effort and commitment needed to ensure actual privacy. The "add water and stir" recipe may be good for the survey results and PR, but not for real privacy.

It would be helpful if industry groups provide full disclosure on their pre-survey efforts to have a better sense on their impact on the Survey, whether big or small. A suggestion for the future is for the FTC to conduct the next surveys internally and on an unannounced date, so as to better measure the natural state of the market rather than a prepared response.

Results: Not Much Privacy

Out of 364 sites observed by the Survey for five elements of FIPs (Notice, Choice, Access, Security, Contact Info):

65.1% had at least one element
54.7% had at least two elements
39.1% had at least three elements
25.8% had at least four elements
9.6% had all five elements observed

These were the results for an 'easy grading' of elements in a partial list of FIPs. If FIPs were measured more tightly, the results would be reduced even below 9.6%. Clearly, there is still a long way before all Fair Information Principles are adopted and practices that provide real privacy are fully established.

Results: Comparing The OPA Survey with The Culnan Survey

As mentioned earlier, the OPA contracted Mary Culnan to conduct a parallel survey of the top 100 visited sites. As also mentioned earlier, the preliminary activity of industry groups to warn web sites and prepare them for the survey makes the results of the top 100 sites almost meaningless in terms of inference to the rest of the Internet.

However, the OPA survey does provide a window to those 100 sites. The most interesting aspect in comparing the OPA Survey (top 100) to the Culnan Survey (top 7,500) is the realization that while the top 100 sites provide more information to consumers, their collection and unauthorized use of personal information is also higher. Thus, the top 100 sites are more likely to collect identifiable personal information (99% vs. 92.9% of the top 7,500 according to Survey question Q1A), use that information for marketing or other secondary internal purposes (83% vs 73% according to Q27) and are significantly more likely to disclose information to third parties (74% vs. 54% according to Q29). The top 100 sites are also a little less likely to commit to not disclose non-aggregate personal information (27% vs. to 30.5% of top 7,500 according to Q30)

Therefore, the surveys show us that while privacy options at top sites increase, the actual privacy of consumers who rely on the defaults of those sites, as most consumers traditionally do, actually decreases.

Results: Misleading Post-Survey Interpretations

After the initial results of the Survey were released, many media stories provided misleading information about the results of the surveys and their meaning. A typical case was a statement that the percentage of sites that post information practice policies rose from 14% in 1998 to 65% in 1999 (as was explained

above, these samples were conducted on different populations and they are hence incomparable). Unfortunately, some of the misinformation was provided by organizations who knew the survey and its finer points intimately. For example, a 5/14/99 press release by TRUSTe (http://www.truste.org/about/about_gtowncomments.html) included the following sentence:

"According to the Georgetown Internet Privacy Policy Study, 94 percent of the top 100 sites have enforceable privacy policies, reaching 98.8 percent of all consumer Web traffic." (last sentence of paragraph four)

This single sentence has four false or misleading pieces of information:
1) As was clearly stated and agreed upon, the top 100 survey is called the OPA survey. The official Georgetown / GIPP / Culnan Survey is of the top 7,500 sites. Yet, nowhere in the release is there anything to indicate that there are two studies with different names and of different populations. Thus, readers are led to believe that this sentence refers to the official Culnan study results.
2) While 94% of sites in the OPA survey had at least one FIP element, only 13.8% had all five elements. Thus, 94% is not an appropriate number, even by FTC or industry standards, to represent good privacy policies, as the release implies.
3) Nothing in the study measures enforceability of the policies. They are only posted policies.
4) The top 100 OPA survey gives reach of 94.4%, not 98.8% which is the reach of 7,500 site universe of the larger study (as stated earlier, both the 94.4% and 98.8 figures are likely inflated because they include portal traffic).

This experience indicates that future surveys should be constructed carefully so as to minimize the chance of confusion and misinterpretation of the results. Further, the conductor of the survey should issue a separate statement to counter anticipated pitfalls with clear discussion (somehow, the inclusion of those statements in the Survey report itself was not sufficient). It would also be helpful if organizations better scrutinize their PR statements to make sure their facts are correct.

Conclusion

Ram Avrahami was a member of the advisory committee to Mary Culnan for the 1999 Internet survey of top 7,500 sites. It is hoped that the comments above help to place in perspective what the Culnan Survey does and does not imply about privacy on the web. I thank Professor Culnan for her efforts and for allowing me to provide input on the Survey.

Ram Avrahami
avrahami@named.org
www.named.org

National Consumers League
Statement on the Georgetown Internet Privacy Policy Survey

What difference does a year make? Not nearly enough. The Georgetown Internet Privacy Survey clearly shows the futility of relying solely on voluntary measures to achieve comprehensive privacy protection. Policy makers should also take note of the fact that it is impossible to assess the effectiveness of self-regulation based merely on the basis of what web sites *say*, rather than on what companies actually *do* with the personal information they collect from consumers.

How much information is collected? According to the survey, 92.9 percent of the sites visited collected at least one type of personal identifying information and most collect several different types. More than half collect demographic information, and a similar number collect both personal identifying and demographic information which, when combined, can be used to paint detailed pictures of consumers' lives.

Yes, more web sites are saying *something* about privacy than was the case a year ago B good news but not unexpected, considering the tremendous effort that many major businesses and trade groups have made in the last year to post privacy information on their sites and encourage others to do so. But while nearly two-thirds of the web sites surveyed have at least one type of privacy disclosure, only 9.5 percent addressed all five of the modest elements of fair information principles that the survey looked for: notice, choice, security, access, and contact information.

This *was* a surprising result, since the Federal Trade Commission stressed the importance of these principles in reporting its own survey findings last year and businesses that participated in subsequent self-regulatory efforts seemed to embrace them. Indeed, the survey graded companies' efforts fairly leniently; instead of looking for specific enforcement mechanisms, the survey gave credit to sites if they simply provided contact information for questions or complaints.

Furthermore, the survey really only shows what some web sites *say* about their privacy practices. To test what actually *happens* to consumers' information, how easily they can *access* it, and how they can *enforce* the proper use of it would require another, much more extensive project. Though the Georgetown survey is only one piece of information that the FTC will consider in formulating further recommendations concerning privacy to Congress, it must be viewed from the correct perspective in the current policy debate.

A survey released on May 19, 1999 by the National Consumers League may shed some more light on the issue of privacy. As part of the "Consumers in the 21st Century Survey" conducted for NCL by Louis Harris & Associates, people were asked about how they thought they would be using technology in the future and how concerned they are about privacy. Eighty-eight percent of consumers said they are somewhat or very concerned about privacy.

And even though a large majority, 76 percent, believe that technology will make their lives easier and more convenient, consumers are still wary of providing sensitive information online. Seventy-three percent said they were uncomfortable providing credit card information, 73 percent were uncomfortable providing other financial information, and 70 percent were uncomfortable providing personal information in general online.

When asked if they had ever had a problem online with fraud or unauthorized the use of their personal information, seven percent of the NCL survey respondents said yes, a figure that represents six million American adults. Seven percent also reported having a problem with fraud or unauthorized use of their credit card information online, 2 percent with fraud or unauthorized use of other financial information online.

One argument that some make for why comprehensive laws to protect privacy are not necessary is that if companies don't live up to the policies they voluntarily state, they can be sued for unfair or deceptive acts or practices. But what about the one-third of companies that don't say anything about their privacy policies at all on their web sites? What about the confusion caused by the nearly total lack of uniformity in companies' stated privacy practices? And what about the fact that a company's privacy policies in the online context might be very different than how it treats consumer information collected offline?

The problem is that there are no basic rules that companies must follow, and that consumers can rely on, to protect privacy. Even the most basic right B the right to be left alone B is not guaranteed in cyberspace. It's hard to be anonymous online, even if you're not making a transaction for which information about you might be needed. And yet in the physical world we expect to be able to browse through a store, leaf through books in the library, or walk down the street looking at shop windows, or pay for something with cash, without having to give someone our names, addresses, or phone numbers, let alone social security numbers or other personal information. Indeed, we would be discomfited at the very suggestion.

And if, as many argue, we benefit when we provide that precious commodity, our personal information, in the marketplace, how do we know if it's a fair trade -- or even that a trade is occurring -- without clear disclosures about whether and how our information will be used? How can we get redress if we think it's a raw deal, or if we never agreed to make a deal, without clear means of enforcement?

Businesses that are sensitive to consumers' inherent privacy rights and voluntarily adopt policies that respect those rights should be applauded. And self-regulatory efforts *are* helpful, as the survey shows, in educating companies about fair information practices. It's also smart for businesses to protect consumers' privacy, though the Georgetown survey shows that only a small fraction of companies "get it."

Let's stop arguing about self-regulation versus regulation -- that's not the point. We know that we will never achieve 100 percent, or even 90 percent, compliance with

basic fair information practices solely on a voluntary basis because not everyone will agree to do the right thing. And we know that enforcement is most effective when there are bright lines of demarcation between appropriate and illegal behavior. Let's move forward by focusing our attentions on how we can create clear privacy rules for everyone to abide by.

An alliance of American companies & associations
committed to protecting individuals' privacy online.

Online Privacy Alliance
Comments on the Georgetown Internet Privacy Policy Study

The Online Privacy Alliance (OPA) welcomes the opportunity to comment on the Georgetown Internet Privacy Policy Study ("the Georgetown Privacy Study"). This important study sheds much light on the status of online privacy and will help guide the OPA's future efforts to advance effective online privacy policies in the private sector.

Over the past year the OPA has worked to expand the adoption of effective online privacy policies by organizations doing business online. Clearly, the Georgetown Privacy Study indicates that significant progress has been made in safeguarding privacy online. The fact that close to 66 percent of sites in the sample posted a privacy disclosure demonstrates that adoption and disclosure of privacy policies is becoming the norm on the Internet. Last year, the FTC reported that only 14 percent of Web sites notified consumers about their privacy policies. Although the universe from which the survey samples are drawn differ, it is very clear that there has been enormous progress.

While much progress has been made, the Georgetown Privacy Study also points to areas where work remains. The OPA's Guidelines for Online Privacy require notice, choice, accuracy, security and contact information. While the Georgetown Privacy Study shows that fewer than 15 percent of sampled sites include all of the elements adopted by the OPA, the statistics for notice and choice are quite high, 87 percent and 77 percent

respectively. The OPA is now directing its efforts to improving the numbers for access as a mechanism to ensure accuracy on contact information. We believe that the 46 percent that disclosed security precautions taken may not reflect actual practice. It is likely that many sites which do appropriately safeguard personal information did not disclose their security precautions in the privacy policy.

The OPA and its supporting organizations will continue to work to ensure that effective online privacy practices are adopted and implemented among the private sector. In particular, we will be focusing on continuing outreach through business and consumer education, while increasing awareness of various privacy assurance programs. The Georgetown Privacy Study will serve as a road map to help us ensure that robust privacy practices are the norm online.

Privacy Rights Clearinghouse - Beth Givens,[1] Director
Comments on the Georgetown Internet Privacy Policy Survey

The Emperor's New Clothes: Privacy on the Internet in 1999

The most irrefutable finding of the May 1999 Internet Privacy Policy Survey (hereinafter called the Survey) is that *collection of personally identifiable information is the norm* on commercial web sites. The Survey found that 93% of the sites in the sample (n=364) collect at least one type of personal information (such as name, email address, postal address). Only 7% of the sites collect no information.[2]

Imagine if nine out of ten of the commercial establishments you visited in the *physical world* were to collect and store information pertaining to your identity[3] – whether you actually purchased something or just browsed, whether you paid by cash or by credit card or check. Imagine if a record were created of the stores you visited, the merchandise you viewed, the books and magazines you perused, as well as the times, dates and duration of your commerce-related activities. You would no doubt have the feeling that your every move was being tracked as you traveled about the commercial landscape. You would also no doubt feel that you have virtually no privacy. Yet, the collection of personally identifiable information has become standard practice on a vast majority of commercial web sites.

The definition of privacy used in these Comments pertains to *control* -- the ability "of individuals … to determine for themselves when, how, and to what extent information about them is communicated to others."[4]

The policy tool that has been created to provide individuals a measure of control over their personal information is the Fair Information Principles (FIP). The principles were first developed a quarter century ago when the U.S. Department of Health, Education and Welfare (HEW) studied the best way to take advantage of the growing power of computers without trampling on personal privacy. A task force of the HEW developed a set of five principles that have since formed the basis of privacy-related laws in the U.S. The FIP have also been codified into the national data protection laws of many industrialized countries (the U.S. is the exception, having pursued a sectoral approach to privacy protection rather than adopting an omnibus privacy protection law).

---

[1] Givens was a member of the Survey's Advisory Committee. The Committee was comprised of 14 individuals from industry, six from consumer and privacy groups, and one from academia. The Privacy Rights Clearinghouse is a nonprofit consumer information and advocacy program based in San Diego, California. http://www.privacyrights.org.

[2] Survey results can be found at the web site of study director, Prof. Mary Culnan of the School of Business at Georgetown University. http://www.msb.edu/faculty/culnanm/gippshome.html.

[3] Granted, a growing number of commercial establishments use video surveillance cameras to make a record of shoppers and employees. But the video systems do not [yet] have the ability to identify those individuals captured on tape. And they are usually destroyed after a short period of time.

[4] Alan Westin. *Privacy and Freedom* (New York: Atheneum, 1967), 7.

The shortened version of the HEW's Fair Information Practices is: openness (no secret data collection), notice, limitations on secondary use, correction, and security.[5] In 1980 the Organization of Economic Cooperation and Development (OECD) expanded on these principles by adopting a set of eight Fair Information Principles. The principles of purpose specification, use limitation, and individual participation were added to HEW's list of five. The OECD principles were adopted by 24 countries including the U.S.

The Survey used a variation of these principles to evaluate the adequacy of personal privacy protection for individuals who visit commercial web sites. The four principles are *notice, choice, access and security* – deemed by the Federal Trade Commission in 1998 as de facto standards for privacy protection on the Internet. A fifth factor, *contact,* was also considered in the Survey's evaluation scheme, whether or not a web site visitor could "ask a question about the site's information practices or … complain to the company or another organization about privacy."[6]

Survey findings are dismal indeed when placed against the backdrop of near universal data collection by commercial web sites.

- Less than 10% of the sites post privacy policies that comprise all five elements of notice, choice, access, security, and contact.
- One third of sites post no privacy policies at all.
- Survey findings regarding data security should be particularly alarming to consumers who wonder about the safety of their personal information collected by commercial web sites (such as credit card numbers). Only 19% of sites disclose the steps they take to safeguard the data they collect and store about their web site visitors.

On a more positive note, nearly two-thirds of sites posted some form of a privacy statement, up from 14% in a similar 1998 Federal Trade Commission study. However, given the fact that over 90% of commercial web sites collect data from their visitors, this finding should provide little comfort to consumers who are avoiding the Internet because of fear that their privacy will be invaded.

Industry representatives have proclaimed this single finding – the increase in sites that post privacy statements – as proof that, indeed, self-regulation can be counted on to protect consumers' privacy on the Internet. This brings to mind the fairy tale "The Emperor's New Clothes." The citizens of a mythical kingdom were duped into believing that the emperor was adorned in the most splendid of garb, when in fact he wore nothing at all.

Unlike the Emperor's loyal subjects, we must not be lulled into believing that the increase in sites that post privacy statements is evidence that consumer privacy protection is assured on the Net. Robust privacy policies are *not* the norm on commercial web sites.

---

[5] See Robert Ellis Smith. *The Law of Privacy in a Nutshell.* (Providence: Privacy Journal, 1993), 50-51.

[6] Mary J. Culnan, Ph.D. "Draft. Georgetown Internet Privacy Policy Survey: Privacy Online in 1999: A Report to the Federal Trade Commission." (Washington, D.C.: Georgetown University, May 13, 1999), 8.

We only need to look at several privacy fiascos of late to realize that the presence of privacy policy statements does little to safeguard Internet users' privacy.

- Some "shopping cart" software, for example, has been found to enable other web users to view shoppers' order information.
- GeoCities, a provider of free web pages, was found to have disclosed information about its members, many of whom who were children, to third parties, even though it is a member of the privacy seal program Truste.
- AOL disclosed information about one of its subscribers to the Navy without a proper warrant, in violation of the Electronic Communications Privacy Act and in violation of its own member services agreement.
- Microsoft's Internet Explorer 5.0 was found to inform web sites when users bookmark their pages without obtaining the consent of those users. Microsoft is a member of Truste.
- The chip manufacturer Intel has released the Pentium III chip containing unique serial numbers that enable individual users' transactions to be tracked in cyberspace.

What have we learned from the Survey, in addition to the fact that commercial web sites have a long way to go before consumers can feel confident that their privacy is protected?

- We must view privacy policy statements in a much broader context. They are but one part of a more complex Internet privacy environment and cannot be deemed as the sole evidence that self-regulation works and that Internet users' privacy is protected.

- We must recognize that the Survey used "easy grading" methodology to evaluate the web sites it studied, something the Survey director explained in the report. Not only were sites given a high grade for simply having a single "information practices statement," but the FIP standards selected to evaluate the content of privacy policies were significantly weaker than the OECD principles that have become the de facto standard to evaluate privacy protection practices.

- If more such Surveys are to be conducted in the coming years, they must move beyond the simply tallying of whether or not a web site has a policy. They must even move beyond counting how many elements of the Fair Information Principles are embodied in individual privacy policies. Consumers' actual experiences in the electronic marketplace must be tracked.

- The Federal Trade Commission, or another appropriate federal government entity, must exert a stronger leadership role in evaluating the adequacy of privacy protection policies and practices in e-commerce.

    - If similar surveys are to be conducted in the coming years for the purpose of evaluating whether or not self-regulation is effective, the FTC or another appropriate federal government entity must sponsor and fund such surveys. Industry-funded surveys cannot be counted upon to present a balanced look at the

adequacy of privacy policy statements on commercial web sites. The amount this Survey cost, approximately $60,000, is a small amount to factor into an agency's budget.

- The purpose of such surveys should be shifted from evaluating the efficacy of self-regulation to assessing whether or not Internet users' privacy is being protected.

- The FTC or another appropriate agency must look beyond a simple tallying of web site policy statements, as indicated above. It should employ more qualitative study methods in the future in order to assess whether or not consumers' privacy is being adequately protected on the Internet. And its standards for determining the adequacy of online privacy policies must include *enforcement* mechanisms and whether or not they provide meaningful redress for consumers' grievances.

TRUSTe
Comments on the Georgetown Internet Privacy Policy Survey

While no direct statistical comparison can be made between the 1998 Federal Trade Commission survey and the 1999 Georgetown survey because of methodology differences, it is clear that significant progress has been made. When TRUSTe launched, nearly two years ago, one of our most significant challenges was to convince Web site owners that privacy was an issue they should put resources toward. The fact that now, 65.7% of commercial Web sites are addressing consumer privacy is a remarkable demonstration that the message has been received, loud and clear. Based on the current rate of enrollment in TRUSTe's program, which has doubled in the last three months alone, TRUSTe is confident that widespread adoption of privacy policies will only increase exponentially. What's more, most of these companies are small businesses; this fact refutes the supposition that only large companies with extensive resources are getting the message.

Again, while direct comparisons are not exact, the FTC's 1998 survey showed that 2% of sites posted "comprehensive" privacy statements, or statements that addressed all elements of fair information practices. The fact that this year, 14.8% of sites posting privacy statements are adhering to fair information practices should not be under-valued. This number is, in TRUSTe's opinion, outstanding. Of course, the ultimate goal is widespread understanding of fair information practices, but when viewed in the context that these elements were not publicly introduced until last summer, the achievement of educating those 14.8% of sites about what fair information practices are in only eight months is a significant accomplishment that should be recognized by government, privacy advocates, and industry alike. In other words, it is significant in and of itself to have educated 65.7% of sites about the need to post any kind of privacy notice. To have also educated such a significant portion of the online world enough that they could achieve the often complex implementation of all fair information practices is remarkable.

Much criticism has been voiced that the online industry has not moved quickly enough to demonstrate that it takes the issue of privacy seriously. TRUSTe believes that, to the contrary, the online world has moved extremely quickly. It is highly unlikely that a two-thirds adoption of such complex guidelines could have occurred as quickly in the offline world.

This is not to underestimate the significant amount of education yet to be accomplished. We must always strive for 100% adoption of fair information practices by Web sites. But TRUSTe's own model clearly demonstrates that it is much easier to educate a site about what should be in a privacy statement once the site has already accepted that a privacy statement is a necessary part of doing business on the Web. When TRUSTe launched, we found it necessary to limit our requirements to full disclosure to convince *any* site to join the program. However, as our educational efforts progressed, we made the decision to raise the bar by adding the other three elements of fair information practices (choice, access, and security) into the program guidelines. Sites have universally stepped up to the challenge as they have renewed their licenses during the last year.

Now that two-thirds of all sites are posting some type of privacy notice, the mission of seal programs is clear—evangelize the need for comprehensive statements that address all fair information practices. Seal programs offer turn-key solutions to sites by ensuring they adhere to all fair information practices prior to granting the seal. What's more, as

the Children's Online Privacy Protection Act is further articulated and refined, seal programs will again assist sites in implementing the complexities of the legislation.

As mentioned above, the increase in number of sites joining the TRUSTe seal program each month is heartening. As TRUSTe predicted in our 1998 Report Card, issued in December, the period of early adoption by innovators was coming to an end and mass adoption was in the nascent stages. This prediction has proven true. During each of the past few months, close to 100 new sites have joined the TRUSTe program. What's more, serious commercial sites now approach TRUSTe very early in their development to gain assistance in developing their privacy policies.

Again, while we can not let the pressure on Web sites to adopt fair information practices subside, the progress report indicated by the Georgetown survey is heartening. Industry is responding to consumer concerns because it's the right thing to do and it's good business.