Statement of eCustomers.com

James C. Allen
Vice President, Development and Operations
eCustomers.com

As a principle of a recently launched, venture-backed start up, it has been a tremendous experience for me to participate in the FTC's Committee on Online Access and Security. It has broadened my perspective and given me the opportunity to contribute towards the resolution of a set of issues I consider critically important to the future of our industry, and to people who use the Internet worldwide. I hope I've also been able to add some flavor of technology "can do" to the challenges the committee has tackled. There are no insurmountable technological barriers to giving people reasonable access to their online data. We've already shown that at eCustomers.com.

Rather, the issues around access and security are ones of the context in which they are implemented and judged; in other words, how they work in a real, day-to-day business environment. Coming out of the experience, here are some brief thoughts to consider in formulating the next steps:

- Different types of data require different levels of sensitivity. The committee's report addresses a wide range of situations, and I would hope that the FTC considers the data gathering context, as well as its application. Some highly sensitive data – for example medical history, social security numbers, and credit-worthiness – need to be approached with rigorous confidentiality. Other data – region of residence, whether someone owns or rents a home, car driven, etc. – is less sensitive. If used appropriately this basic marketing information has the potential to transform the Internet into a vibrant, humanized medium for e-commerce. For example, we use anonymous data scores to personalize web site content. This application should be judged very differently from one that includes sensitive data.

- Technology is neither good nor bad. The issue is how the technology is used, and whether its use is acceptable to everyone involved. Technologies like cookies offer an e-marketing company the tools to make the consumer's online experience as powerful and memorable as any on-land shopping experience – and more convenient and less time consuming. This is a good thing for business and consumers, and by fueling the economy, it is ultimately good for society. This is not to underplay the importance of responsible action. E-marketers must act as trusted agents, keeping the consumer at the center of their development and marketing philosophies.

We are operating on the leading edge of a business revolution. There are few guidelines to use to make balanced decisions. The FTC and organizations like CDT, EFF, EPIC, and others have helped by raising the issues. Increasingly, the Fair Information Practices are being used as an international platform. However, technology continues to evolve and the business environment remains volatile and opportunistic. As businesses, we must be prepared to evolve and adapt while we honor basic ethical guidelines, keeping our customers, partners and key constituencies apprised of any changes in our plans and policies. In the meantime, we must continue to push the Fair Information Practices as far as they can be implemented and probe how we can better inform consumers about our practices and our implementations of technology.

May 11, 2000

Concurring Statement of Stewart Baker, Steptoe & Johnson LLP

I fully concur in this report. Indeed, I am proud to be part of the Committee that produced it. The Committee included practically every stripe of opinion, yet its debates were always respectful and, against the odds, they produced at least partial consensus. That said, I write separately to point out the strict limits of our consensus on security, the serious nature of the issues that prevented us from reaching a similar consensus on the access question, and the lessons that should *not* be drawn from this report.

***

First, security. Our recommendation on this point is made in the context of voluntary action by commercial Websites. In other words, these are things that responsible Websites should consider implementing as a matter of good business practice. There was no agreement on government-mandated security standards, and in particular no agreement that the FTC should be more heavily involved in setting standards in these areas.

Why not? Well, first because the FTC, like this Committee, lacks the necessary jurisdiction. The FTC may have authority over commercial Websites. But as the report also notes, the risks to personal information are not restricted to commercial Websites. In fact, the risk of a data compromise may be worse on, say, political Websites that gather both credit cards and sensitive political data about individuals. What's more, every business in America gathers some customer information, including a large volume of credit card numbers. The security of personal data is not a problem limited to Web sites. If the issue requires regulation, we should impose security programs on every bookstore and restaurant and dry cleaner in the country that handles credit cards and other personal data.. We certainly should not make "Regulate the Net First" our slogan.

Even if we decided to focus only on Internet security, the FTC is not the place to address the issue. Exposure of personal data from Web sites is not the Internet's biggest security problem – not by a mile. The Committee did not hear any evidence that consumers had actually suffered significant losses from exposure of their personal data on the Internet (it appears that losses from the well-publicized hacker thefts of credit card information fell mainly or exclusively on merchants and banks). Yet at the very time the Committee was meeting, Web businesses were cut off from customers by denial-of-service attacks, and the Committee's own deliberations were disrupted by a global computer worm. If a handful of script kiddies and a second-rate computer programmer can do that much damage, hostile nations employing talented computer scientists can do far worse. In the long run, these security issues will be more important to Americans than protecting their shoe sizes or even their credit card numbers from voyeurs.

So, before rushing forward with legislation or regulation to solve what may be the least significant of the Internet's security problems, we need to look at Internet security from a much broader perspective. This, of course, is an inquiry far beyond either the FTC's experience or its expertise.

Next, the access question. It sounds like a good idea for consumers to be able to see the data that Web sites have assembled about them. In fact, it is a good idea, but one with clear limits. We heard estimates from Web companies that less than one percent of customers who are offered access actually take advantage of the offer. (That sounds about right. Ask yourself whether you've exercised your access rights recently. If you're like me, your answer is, "Hey, life's already too short.") But maintaining a system to satisfy the most curious one percent of American consumers could be quite costly, and the costs would be borne almost entirely by the other 99%..

And financial costs are the least of the problem. Far worse is that, as the Report says, "Giving access to the wrong person could turn a privacy policy into an anti-privacy policy." If access to personal data is turned into a legislative right, Americans' personal data will be at risk of exposure to con men, private investigators, suspicious spouses – anyone who has the *chutzpah* and the scraps of information needed to plausibly impersonate their target.

That's bad for all of us, but it is especially bad for the companies forced to set up some sort of access system. If they demand clear and convincing proof of identity before releasing personal data, they will be accused of offering access in theory while denying it in practice. But if they relax the rules, they will surely be sued every time a con man exploits the relaxed rules to steal a consumer's identity.

This "damned if you do, damned if you don't" liability problem makes it particularly clear that the FTC has no business imposing an access requirement on its own, not even in the context of consent decrees and other quasiregulatory programs. Why? Because if society chooses to require access – and to accept the risk of improper disclosure that goes with it – then surely it should protect from liability the businesses that comply in good faith, even if the access is abused by fraudsters. Unless the FTC can protect companies against the liability risks that go with consumer access, it should not demand that they throw themselves into harm's way.

***

Finally, a word in closing about the use that will be made of this report. Although the FTC completed a "sweep" of Internet sites and privacy policies during the Committee's deliberations, it refused to share that data with the members of the Committee. Too confidential, we were told. But on the day our report was put to bed, details of the "sweep" were leaked to the press and Congress.

That was unfortunate, but what was worse was the way the sweeps study – which we still have not seen -- apparently ignores the lessons of this Committee's report. If the leaks are to be believed, the FTC's sweeps study acknowledges that many more Web sites have privacy policies than even a year ago, but it criticizes the Web sites' policies for not including access and security elements.

The lesson of this Committee's report, however, is that neither of these elements needs to be part of every Web site's privacy policy. Of security notices, we said: "Since it is difficult to convey any useful information in a short statement dealing with a subject as complex as the nuts and bolts of security, most such notices would be confusing and convey little to the average consumer. Further, providing too many technical details about security in a security notice could serve as an invitation to hackers."

On access, of course, there was no agreement. But many of the Committee members thought that providing access to Web site data was often unnecessary. Two of the four options reflect a view that access is worth the cost mainly when it allows consumers to correct information that could hurt them if left uncorrected – credit reports, school transcripts, and the like. But most Web sites don't collect information for those purposes. More commonly, the data is maintained for the purpose of knowing more about their customers' likes and dislikes, or for advertising demographics and tailoring, and so on. The data may also be mixed with proprietary and third-party information that should be protected. In those circumstances, it's quite reasonable to conclude that no consumer access is appropriate. Certainly that is a view that falls well within the range of options laid out by the Committee.

In short, many Web sites do not provide access to personal data for reasons spelled out in the report of the FTC's own advisory committee. These are not shady businesses that must be brought to heel; they are part of the mainstream and they are often acting quite reasonably. To criticize such Web sites for lacking an access policy – or to suggest that the FTC needs to step in and solve some kind of "access crisis" on the Web -- is to ignore the lessons of this Report.

Individual Statement of Richard Bates, Vice President Government Relations, The Walt Disney Company

I would like to say at the outset that it was a privilege and honor to serve on the Advisory Committee on Online Access and Security. The Members of the Commission and the F.T.C. staff should be commended for their hard work and the commitment that went into the final report.

Nevertheless, since the explosion of the internet economy, the efforts made by industry with respect to self-regulation on privacy matters has not been given its proper due. Mandatory privacy legislation appears to be politically popular at this time. However, the siren call for privacy legislation could have disastrous effects on an industry that is fueling our economy, creating millions of jobs, and bringing the world closer together.

Burdensome federal regulations dealing with privacy, and what could be worse, 50 individual state privacy, and security laws would clearly kill the golden goose. Self-regulation with respect to privacy can work if given time. Consumers can make informed decisions if given the tools to do so. It should be the responsibility of the internet community to make sure consumers have the tools to make decisions with respect to privacy, and I believe the industry has and will continue to work towards this goal.

Again, this has been a great experience and it was my pleasure to work on the Advisory Committee.

Statement of Fred H. Cate

Professor of Law, Harry T. Ice Faculty Fellow,
and Director of the Information Law and Commerce Institute
Indiana University School of Law—Bloomington

From the first announcement of the Federal Trade Commission's intention to create an Advisory Committee on Online Access and Security there has been some ambiguity as to whether the Committee was intended to make specific recommendations or whether it was merely to identify options for future Commission action. Ultimately, the Advisory Committee decided to pursue only options, with the one exception of single recommendation concerning security. On no other matter was any consensus formally measured or sought, and at no time was any substantive vote taken, other than the vote to transmit this final report to the Commission.

The members of the Committee, the Commission, and the public might wish that we had reached a consensus or provided more indication of the level of support among the Committee members for the various options outlined in our report. But we did not. What we did accomplish, however, is not insubstantial: The report provides a valuable catalog of options concerning online access and security. It highlights the serious need for further research in this area. And it amply illustrates the complexity and significance of these issues. That may frankly be the Committee's and this report's most significant contribution: We have thoroughly demonstrated the extraordinary complexity of even this small subset of privacy issues.

Even so, as the final section of the report makes clear, there are many issues that we did not address because they were beyond either our charge or the time available for our deliberations. Noncommercial, government, and non-U.S. web sites are not included, even though they arguably constitute a majority of sites on the web today. We largely ignored access and security issues in contexts other than online. We did not reflect on the expanding volume of self-help and self-regulatory measures for protecting privacy online, nor on the extensive practical experience and litigation involving implementation of the access and correction requirements in the Privacy Act, Freedom of Information Act, and similar state statutes. Had we done so, this report might have looked very different, and our understanding of the potential risks and costs involved in providing access and an opportunity for correction enlarged. To be sure, had we addressed all of those issues, this 16,000-word report would have reflected even more complexity and an even greater range of views.

I join my colleagues in acknowledging what a privilege it has been to serve on the Advisory Committee. The breadth and depth of knowledge reflected by the members were impressive; there was never a meeting that I did not feel that I was learning vastly more than I could possibly be contributing. I also want to add my personal appreciation to the Federal Trade Commission staff who supported the Committee's work. They were tireless, merciless, and invaluable. The Committee was, and the public continues to be, well-served by their skill, professionalism, and commitment.

SEPARATE STATEMENT OF JERRY CERASALE
Concerning the Report of the Advisory Committee on Online Access and Security

It was a pleasure to be associated with all the members of the Committee, and I thank the Federal Trade Commission for allowing me to be a member. I must commend every member for the difficult and time-consuming efforts required of each of us--efforts that far exceeded my expectations.

I must raise a serious concern about the process of the Committee. At our first meeting we had discussions on the Web sweep being conducted by the Commission and whether or not the sweep should be delayed until the Committee issued its report. The sweep, of course, was not delayed. Unfortunately, some of the fears expressed by proponents of delay may have become a reality. **Before** this Committee has even issued its report, it appears that the Commission staff has recommended rulemaking action based upon Web sites failing to provide access. There is no consensus in this report for any government action. Access is a very complicated issue, and any recommendation for government action a few weeks before or after the report is issued likely was determined before our Committee spoke.

Commerce conducted, at least in part, *via* the Internet is growing. The majority of state Governors have expressed to Congress significant concerns over potential loss of sales tax revenues due to increased remote sales over the Net. The National Retail Association has told Congress of its members' concerns that American tax policy favors e-commerce, which in turn poses a threat to retailers. Internet sales are projected to grow rapidly in the near future. Moreover, technology is changing--broadband to all homes, for example--which will enhance the e-commerce experience. Internet sales are here to stay.

The only thing on the horizon to dampen the growth of e-commerce is ill-conceived government intervention. My biggest fear is that privacy legislation may have that effect. The Internet is an open marketplace with few barriers to entry. A significant and costly privacy regime, particularly access requirements, placed on the Net will become a huge barrier to entry. First, new companies would have to establish, maintain and operate procedures to provide access. Second, new companies would find it very difficult to find prospects for their offerings.

Access must be reasonable and must be based upon the use of the data. There is a significant difference between using data to determine a consumer's eligibility for a good the consumer wants and using data to determine whether or not a business will spend its resources to market a good or service that the business believes will interest the consumer. I do not believe that the report places a proper focus on how information is used.

I found it difficult to decide whether or not to support the report, in large part, because the Commission staff has recommended immediate regulation on access provisions. The report does not call for regulation or legislation. I am confident that the Commissioners will recognize that, and for that reason alone I will support release of this report.

Statement of Mary J. Culnan

Professor, McDonough School of Business
Georgetown University

I am honored to have had the opportunity to serve as a member of the FTC Advisory Committee on Access and Security. As our report demonstrates, these two elements of fair information practices present a number of policy and implementation challenges. My comments address needs for empirical research related to the Advisory Committee's work: the relationship of notice to access and the need for empirical research on what elements make privacy disclosures useful to consumers.

First, access plays an important role in promoting transparency. In 1973, the first principle of fair information practices was that there should be no secret systems: individuals should know what personal information organizations hold on them. Obviously, one way to provide this accountability is for individuals to see the information that organizations hold about them. However, as our report demonstrates, providing this level of access can be difficult or prohibitively expensive.

When personal information is used to make important decisions about an individual, the individual should clearly have the right to see the information and to correct errors. However, for information that is used for other purposes, the individual's interests might be satisfied by better notice: what data elements are kept and how they are acquired, accompanied by a sample record similar to the data cards provided by direct marketers. Empirical research is needed to understand the appropriate balance between notice and access, and to determine under what circumstances this type of disclosure would address consumers' need for transparency.

Second, there is a more general need for empirical research into the elements of effective notice for all elements of fair information practices. For example, our report highlights the importance of notice about an organization's security procedures as well as the difficulty in making such notice both understandable and informative.

Information age marketing no longer consists of a single exchange where consumers exchange money for valued goods and services. Because so many details of the "first exchange" are recorded today, online transactions in particular also consist of a "second exchange" where consumers also provide personal information in exchange for value the organization provides to them (e.g. personalization)[1]. There is an extensive body of empirical research on labeling related to the first exchange (e.g. content and placement of product labels). Privacy disclosures are the equivalent to "product labels" for the second exchange. Research is also needed on what makes these disclosures effective. Just as labels on food products with healthy ingredients may encourage a consumer to purchase that product, effective privacy "labels" may encourage consumers to be more willing to disclose personal information because the risks of the "second exchange" have been reduced.

[1] See Mary J. Culnan and Sandra J. Milberg, "The Second Exchange: Managing Customer Information in Marketing Relationships," July 1998, available at: http://www.msb.edu/faculty/culnanm/research/jm0798.pdf

Statement of Daniel E. Geer, Jr., Sc.D.

CTO, @Stake, Inc., Cambridge, Massachusetts
President-Elect, USENIX Association, Berkeley, California

The first point is simple. In fact, the first point is to be simple. Though the real world is complex and one size of anything never fits perfectly, especially a "one size" of rule-making to provide fairness for folks that don't care that they don't know that they don't have it, the more the rule-making attempts to actually capture the richness and complexity of the real world the more likely its protections are an affected illusion — the promise of a regulation is inversely proportional to its length. Why? Because complex systems fail complexly. We are not designing air traffic control here; we are designing "Thou shalt not kill." If everyone and everything that isn't "too dumb to live" can understand the rule, then it might just have a fruitful effect. If that's not the case, the rule will just amount to a full employment act for those skilled enough to hire themselves out for rule evasion services.

Second point: Stern rules create stern costs; this is only natural. If, however, these stern costs tax day-to-day operation rather than taxing exception handling, then the sterner those rules are the fewer will be the entities that can bear the overhead. At the limit, i.e., if the rules are stern to a fault, then the rules themselves will consolidate data to those few repositories really competent to comply with the stern-ness of the rules. This is the wrong direction. As anyone who handles data classification knows, the dearer the data the more finely you compartmentalize it — unless you can't, but if you can't compartmentalize then you can only fall back to walled compounds with perimeter control and zero sympathy for data sources. The point: Too stern a ruleset and you kill all but those few players most equipped to evade the rules and/or mold the rulemakers. At all costs, avoid regulations that fully consolidate data as regulators inevitably merge with the monopolies they themselves create.

Point number 2 1/2: Security technology can deliver any degree of sterness you want but at the steep end you get a culture of surveillance even if, paradoxically, the purpose of the rules is to avoid a culture of surveillance. Rather than take a security approach take a risk management approach. In other words, instead of turning to technology for proof, especially proof of unavoidable compliance, turn instead to removing the "profit" motive from the outcome you don't want. Note that "profit" can mean infamy as easily as cash in the sense used here, i.e., whatever excites your opponent.

Thirdly, be clear about what you would call "success." The practice of Constitutional law has long had this divide: the framers of the Constitution said "do this" while implying "so we can get that" but how to "get that" has changed over time. Constitutional briefs divide into those that urge timeless loyalty to "do this" and those that urge timeless loyalty to "get that." The churn rate of technology is too fast for the contemplative process of "advise and consent" to keep up and so regulator actions will henceforth never be engaged before considerable private investment is already sunk. Coupled with the boundary-less-ness of the Internet, regulators will henceforth always be looking at horses that are not only already out of the barn but already down the road in some other regulator's jurisdiction. In such a milieu, means are not durable enough to deserve loyalty — only goals are durable. In the detail that matters here, regulation that attempts to out-and-out delay technology deployment might arguably "succeed," c.f., cryptographic export controls, but such regulation will never deny the technology to those who declare that they are ready for it. In short, the unintended side effect of a protection approach will be to widen the gap between technology haves and have nots, as if that trend needed any acceleration. Deliver us, please, from making the cynics the seers; deliver us from regulation that produces ever greater work factors for regulators.

Fourth, the power of a communication network is proportional to the square of the number of nodes (known some places as "Metcalf's Law"). Whatever the inherent value of data, once it is on a network that value is multiplied by the square of the number of parties who might partake of it. If the value of this sharing is a net positive, all the better. However, sharing data against the wishes of the subject has a cost that also rises with the square of the network size into which it is released, and that

cost can never be mitigated because data is never un-revealed. So long as a non-zero dollar value can be established for losing control of a single datum, any finite tolerance for risk establishes an upper bound on the size of the network against which that datum can be exposed. The observed Internet doubling time of six months means that "revelation risk" rises by an order of magnitude every 20 months even if the data at risk are not themselves growing more valuable — which they most assuredly are as business-to-business electronic commerce leaves business-to-consumer forms in the dust.

Fifth, in a virtual world the appreciation of reputation capital drives the appreciation of market capital(ization), not the other way around. Because reputation capital has no mass, the time constants of changes to its momentum and the time constants of deliberative processes like regulation have no relation to each other whatsoever. Regulators will have neither the power to reward nor the power to punish to the extent the capital markets can, do and will. As such, it will be up to regulators to amass enough reputation capital of their own if their pronouncements are to affect the reputation capital of others, i.e., in the parlance of finance, if the regulators are to get traction and to have leverage. This is especially true of crafting regulation where the body of experience is infantile, yet, paradoxically, the body of experience is most infantile precisely at that leading edge where habits and investments are still the most malleable. This is a variation on "Technology is characterized by those who understand what they cannot control and those who control what they cannot understand." These observations are neither pleasant nor fashionable, but they are nonetheless true.

While these few paragraphs are far, far from all that could be said, they say:

Be simple or lose from the get go
Rules that collapse the number of players are too stern
Suppressing technology widens technology divides
Network effects make all other costs immaterial
Market messages are the messages that drive

When a government cannot protect its citizens, its duty is to arm them.

Statement of Rob Goldman

Executive Vice President, Customer Experience
Dash.com

It has been my pleasure and a distinct privilege to serve as a member of the Advisory Committee on Online Access and Security (ACOAS). I have been consistently impressed with the members and organizers of this committee, both in the depth of their thought and in the thoroughness of their deliberations on this important issue. I am especially impressed with the commission for their choice to include representation from small entrepreneurial startups like Dash on the committee. I am honored to represent the perspective of all Internet startups that have gone out of their way to find new means of protecting the privacy of their customers.

The committee was charged with advising the FTC on ways that commercial websites could provide "reasonable" access and "adequate" security for personally identifiable information. The statement that follows represents both my personal opinion and that of Dash on several issues that were not appropriate for inclusion into the committee's final report, but which we feel are crucially important nonetheless.

By what means should the FTC encourage business to adopt Fair Information Practices? Although beyond the scope of the committee's report, this is by far the most pressing unanswered question. In its 1998 paper on the Principals of Fair Information Practices, the FTC lists as the final principal, that of "Enforcement / Redress". They say: "It is generally agreed that the principals of privacy protections can only be effective if there is a mechanism in place to enforce them". I for one concur with the commission's conclusion and suggest that the most effective mechanism that we have for dealing with these complicated issues is self-regulation and the free market.

Working on this committee has been an education in the difficulty that arises when important fundamental principles come into conflict with each other. Many of the basic tenants of Fair Information Practices can undermine each other. The committee has detailed in its report situations where access can be a risk to security. Indeed, without proper authentication, access itself can be a risk to privacy. Perhaps more troubling, Fair Information Practices can, at times, conflict with fundamental principles of good business. Trade secrets, differentiation, and competitive advantage are among the most basic concepts American business, and over and over again we have seen situations where certain types of access or security, if required by law, could undermine good business. This is particularly the case with derived information, which if provided to consumers could at the worst reveal proprietary algorithms or trade secrets which form the basis for a viable business.

As if this complexity were not enough, add to it the fact that the technological underpinning of the Internet industry is shifting constantly beneath our very feet, making it nearly impossible for business to assemble an accurate estimate of the costs of access and security. If these principals were to be legislated or canonized in regulation, then on the margin, consumers would certainly compromise variety and choice in the marketplace in exchange for privacy.

Dash believes powerfully in the right of consumers to have access to the personal information that companies collect about them. We feel that it is vital to the long-term success of our company, the viability of our business model and the vitality of the Internet as a medium. We have gone to great lengths to design a system that allows our customers to have access to the personally identifiable information that we collect about them. We provide this access in real time through our website. We have done this because our customers have demanded it, not because regulations have required it, or Congress has legislated it. In many ways, Dash is the best example of the market working effectively. True, all companies will not necessarily follow in the path that Dash has blazed, but I argue that they need not. Consumers will be the final judges of these matters. They will speak as they always have with their dollars. The FTC need only require that businesses be honest with them, a power which is already granted to the FTC under its jurisdiction in "unfair and deceptive" trade practices.

Given the current vitality of American business in general and the technology sector in particular, it is worth investigating the extent to which the business climate in America has contributed to that success. Certainly it is impossible to credit any single factor with the vitality of and breadth of innovation that America has seen on the Internet. Partially it is the spirit of the American entrepreneur, partially the abundance of capital, partially the size of the market, and partially it is the environment as determined by the government.

From Dash's perspective then, self-regulation is the best path to the widespread adoption of Fair Information Practices. Should the commission choose differently, though and decide to work through government regulation or legislation, Dash will comply happily. For in the final analysis, we are sure that Internet business cannot survive without firmly protecting the privacy of the consumer.

Rob Goldman
May 12, 2000

Statement of Dr. John Kamp, Senior Vice President
American Association of Advertising Agencies

Amid all the legitimate but difficult public policy discussions surrounding the issue of online privacy, participation in this Advisory Committee was an enriching and satisfying learning experience. I trust that those who carefully read this report will agree that both access and security are much more complicated than the press and many commentators would have us believe. Great thanks go to my fellow members for introducing me to these complexities and forcing us all to look beyond our otherwise narrower perspectives.

I write separately to state my perspective on a few points:

1. Both access and security require much more study and public debate before either technologists or policy makers are to make lasting decisions, much less laws or binding rules. Indeed, the most important contribution of this advisory committee was to shed light on the questions, while merely pointing at solutions. While the discussion continues, we would do well to adhere to the "Safe Harbor" principles already well articulated by the U. S. government in international discussions.
2. Although every member agreed that access is a significant goal, its price is not yet fully understood. Access will be expensive in many ways and consumers will bear that expense either directly or indirectly. Let's be very careful before we load expenses on our citizens.
3. Access and security are often in tension. The more access is enabled, the more difficult it will be to maintain adequate security systems. We must balance these goals carefully to give the security experts a fighting chance against the hackers and the snoopers.
4. Not all data require the same level of scrutiny. Existing and evolving laws for health, financial and children's data are not appropriate templates for mere marketing data, especially where consumers have clear notice and choice.

So, as we celebrate the great strides made by the online industries on the issues of notice and choice, let's be very careful to further explore and debate these much more complicated issues of access and security before recommending legal action. Indeed, as if to sober those of us most actively demanding immediate government action on these issues, the "love bug" killed the final drafting process of this report for a critical 24 plus hours. Our frantic final days of editing reinforced the warning of our security experts that there is no such thing as perfect security, only a careful security process.

I was honored to have a small part in this beginning of the process of public debate enabled by the Federal Trade Commission. Thank you FTC staff and commissions, and thank you fellow members of this commission.

Statement of Rick Lane
Director, eCommerce & Internet Technology
United States Chamber of Commerce

It was a pleasure for me to be able to participate as a member of the Federal Trade Commission's Advisory Committee for Online Access and Security. I found the discussions amongst the Committee members to be quite informative. I would also like to thank the staff of the Federal Trade Commission and my other Committee members for making this experience enjoyable.

E-commerce and the use of the Internet is no longer a pet-project of corporate IT departments. It is increasingly becoming a make or break proposition for businesses throughout the world seeking to maintain a competitive edge. E-commerce as a business proposition has clearly turned the corner from a novelty to a competitive reality led by business to consumer and now by business to business commerce. The development of e-commerce has taken place at a heady pace, stimulated by the ability of entrepreneurs to compete in a remarkably free marketplace. As the e-commerce market makes the transition from the early hyper growth stage to steady long-term growth it will require a framework that stimulates innovation and private enterprise and minimizes cumbersome government regulation.

The Internet has dramatically changed the public policy debate. It is impossible to apply old legislative or regulatory paradigms to the new economy without crippling its incredible growth. As the report shows the issue of online access and security is far too complex and moving too fast for government regulators to fully grasp and foretell the negative implications that regulations may have on this dynamic sector.

It can not be emphasize enough that the Internet has given consumers a powerful new tool. At no other time in history has the consumer been in such control over their economic domain. On the Internet consumers determine the price they are willing to pay for products through auctions and reverse auctions and the hours they want to shop. Most importantly, they have the power to ensure that the service they receive from a business is satisfactory, including the use of their personal information, or with the click of a button they are gone to a competitor.

This new consumer power is why we strongly believe that self-regulation of privacy is more efficient and effective than legislation. Businesses understand all too well that if they are not providing a customer with what that customer needs in regards to their privacy, there are thousands of other web sites that will.

What does all this mean to the future of our economy and consumer privacy? It means that that the efficiencies of e-commerce transactions will bring about greater economic growth and provide better protection of consumer privacy through market forces and technological innovation.

Businesses fully realize that in order to build a business on the web they must instill consumer confidence. This cannot be done through legislation, but by proactive steps taken by business to ensure that the use of an individual's information is protected and used in a manner consistent with the expectations of that individual.

STATEMENT OF GREGORY MILLER & MEDICALOGIC INC
CHIEF INTERNET STRATEGIST & DIRECTOR GOVERNMENTAL AFFAIRS

I thank the Federal Trade Commission and MedicaLogic for granting me the opportunity to serve on the FTC's Advisory Committee on Online Access and Security. It has been an honor, a pleasure, and a tremendous experience to serve. It has enlightened my perspective and afforded me a chance to contribute to the development and resolution of one of the most important issues in the third age or so-called digital economy: the privacy of, access to, and security of consumer information. At MedicaLogic we've learned the incredible responsibility we have to serving and protecting the consumer's best interests in the privacy of their health information. As the only healthcare industry participant, MedicaLogic appreciates the great "cross-pollination" experienced in this exercise.

The online world of the digital economy enables the gathering and analysis of consumer information in ways possibly never imagined prior to this Committee's investigation. While we must leverage best practices and principles already before us in terms of fair information practices, we must likewise appreciate the near boundless potential of the Internet medium and move cautiously and judiciously in structuring future public policy, law, and regulation. In general, given the infancy of the digital economy, it is imperative to bear in mind that in shaping law and regulation, less may be more.

The principles of notice, choice, and access are equally important in the compilation of personal information. Consumers should be notified of information gathering practices and policies whenever they use an Internet service, and where appropriate and practical, given the choice to participate in advance of such gathering. Such personal information gathered by business should be accessible to consumers. Applying these three principles with equal force and meaningful standards for each empowers the consumer to take an active role in protecting their own identity and uses thereof. Notice, choice, and access serve as safeguards against overreaching data collection.

Further, it is equally imperative to develop commercial policies and guidelines (whether through preferable industry self-regulation or government mandated guidelines) that business can implement in the ordinary course of commerce. As a result, there may be instances where limitations on notice, choice, or access must be established. When such limitations must be set, it is imperative that the values for such limitations are clearly articulated and narrowly constructed. Most important, such limitations must directly advance a particular public policy.

Finally, privacy and security have a symbiotic relationship and despite conventional technical wisdom this Committee made a case that tension doesn't necessarily exist between them. It is clear we cannot have competent privacy policies without carefully addressing security means by which privacy may be ensured. The majority of my contributions to this Committee lie in the security area. To the extent security is addressed within the context of our charter, the Final Report best reflects my opinions on the matter. However, I add the following point.

Ensuring consumers' access to personal data held by online business entities could actually increase privacy risks unless means are provided to "authenticate" that the requesting entity is, in fact, the individual they claim. This goal must be achieved in a reliable, simple to use, and cost-effective manner. Developing a system to enable individuals to conveniently view (or correct) their personal data can also increase vulnerability to penetration or manipulation of others' data to which the individual does not have authority to access. Accordingly, consumers must be simultaneously empowered to access their own data but prevented from improperly leveraging that access.

Respectfully submitted 11th May 2000.

/s/ Gregory A. Miller, FTC ACOAS Committee Member, gam@gmiller.com

Statement of Deirdre Mulligan, Staff Counsel
Center for Democracy and Technology

It was an honor to serve on the Federal Trade Commission's Online Access and Security Advisory Committee. The individuals assembled represented a diversity of views, expertise and experience. This diversity greatly enhanced the breadth and depth of the Committee's deliberations and our final report. I believe that the report fairly represents the discussion and provides a useful framework for analyzing various options for crafting access policies. However, I suspect that many in the government, the industry, the advocacy community, and the public are seeking advice on what to do, not just an articulation of the myriad choices they have. Therefore, this statement represents my opinion as to how the principle of access should be implemented by commercial Web sites.

Personal information in the hands of businesses should be accessible to consumers. By ensuring that consumers are fully aware of the data that businesses collect and use, access enables consumers to play an active role in protecting their own data. Access serves as a check on overreaching data collection by businesses. Access enables a private force of individual citizens to police the privacy policies of businesses at no cost to the public coffers. Access allows consumers to ensure that data about them is accurate, and perhaps, that it is used in ways that advance their interests.

Consumers have an interest in accessing personal information businesses hold about them regardless of the medium of collection (online/offline), the source of collection (the individual/third party), the method of collection (passive/active), the type of data (factual/inferred and derived), and whether it is tied to offline identifiers or their online equivalents.

There may, however, be instances where we set limitations on access. Throughout history, privacy and other important values have coexisted. Similarly, the principle of consumer access coexists with other important public policy considerations. At times, values conflict. It is important that limitations on access, like other important values, be clearly articulated, narrowly drawn, and directly related to the advancement of a specific public policy goal. This approach is similar to that taken in First Amendment jurisprudence – even where a compelling interest is articulated, it must be advanced in the least restrictive manner possible. In essence, if a compelling public policy interest is in conflict with access, then it must be advanced in a manner that least interferes with the individual's ability to access her information.

I believe that the "default to consumer access" approach articulated in the Report most closely reflects this construction. It both creates a clear presumption in favor of consumer access and allows for consideration of competing public policy interests. This is consistent with existing privacy laws, creates a clear rule that can be understood by consumers and implemented by businesses, and fosters individual privacy by providing individual's with access to information that others hold about them.

Statement of Deborah Pierce, Staff Attorney
Electronic Frontier Foundation

It has been an honor to serve as a member of the FTC Advisory Committee on Access and Security. The diversity of opinions and the experience of the committee members contributed to a full discussion and debate of these issues. I appreciated the efforts of all of the members to include and debate the wide range of options that access and security issues present to us and to then winnow those options down to those that were reasonable. I would also like to thank David Medine for his help in facilitating our meetings with such good humor and grace.

The purpose of our committee has been to provide advice and recommendations to the FTC regarding implementation of fair information practices, specifically by providing the FTC a menu of options for what constitutes reasonable access to personal information by domestic commercial Web sites and what constitutes adequate security of that information. I believe our report has done that.

As a privacy advocate, I feel it is important to remember some of the underlying reasons why codes of fair information practices were first developed. Keeping these reasons in mind is helpful particularly when we try to determine what types of access consumers should be granted in records about them held by private corporations.

These codes, as refined over the last twenty-five years are based on several core principles, including the notion that those who would collect and use personal information have a responsibility to the person about whom the information is about. Because of this, the codes were developed to prevent secret personal data record keeping systems. In addition, the concept of access was developed so that an individual could have the ability to correct or amend a record that contained personal information about that individual.

Based on those concepts, I believe that the total access approach option best captures the spirit in which fair information practices were first developed. Under this approach commercial Web sites would be required to provide access to all of the personal information that is gathered about an individual. This promotes the openness of record keeping systems that fair information practices were designed to achieve. While there may be some drawbacks to this option, I believe the benefits far outweigh the costs. In a climate where individuals are fearful of intrusions of their privacy on the Internet they will be able to see exactly the information that corporations are collecting about them and correct and amend that information if they feel the need to do so.

Allowing for the broadest access to individuals about personal information that is kept about them will, I believe best promote e-commerce in the long run as trust is built as well as protecting individual privacy online.

Individual Statement of Ronald L. Plesser

I last participated in an Advisory Committee twenty three years ago when I was general counsel of the U.S. Privacy Protection Study Commission. This time I was one of forty two members. Back in 1977 the personal computer had just been invented. This time we have the world wide web and a level of interactivity that we could only have dreamed of in 1977.

The issue of Access has not changed much since the Privacy Commission days. The interests of consumers and those who hold records about them remain much the same. The security and encryption issues have changed significantly.

The report reflects options for the implementation of access and security. It does not reflect the strides in self regulation and the need to allow the uninhibited growth of the internet. It is my concern that this report not be seen as a call for mandatory legislation or regulation that will make it more difficult for the internet to develop free of unneeded burden.

Access is an important concept, but it is not the fundamental issue raised by fair information practices. That issue to my mind is “Notice”. Notice provides the knowledge and transparency that is necessary for a consumer to make informed decisions. The more technical and difficult requirements of reasonable access should not take away from or limit the quality and breadth of Notice.

It was my pleasure to have served as a member of this Advisory Committee in the year 2000.

Dr. Larry Ponemon, Partner
PricewaterhouseCoopers, LLP
Member of the Online Access & Security Advisory Committee

"Our present problems cannot be solved at the level of thinking at which they were created."
Quote: Albert Einstein

It has been an honor to serve on the Advisory Committee on Online Access and Security of the Federal Trade Commission (FTC). First and foremost, I commend the Committee for presenting and debating a plethora of important issues and options contained within this important report. At an early stage in the Committee's life, some members of the Committee (including myself) discussed the need to develop a normative or "ethical" framework for guiding our judgments on the fundamental qualities of access and security for consumers in the online universe. My belief is that without a normative perspective, the options contained herein are merely a list of issues rather than a coherent strategy for improvement. As can be gleaned from our public conversation, the tide of discussion moved very quickly to technical or legal description. Following are a few normative areas about online access and security that demand further consideration by the FTC, other Government Regulators, and the United States public at large.

First, access and security alone are not fundamental principles by themselves. In essence, they are ways to engender transparency and stewardship by entities that collect, disseminate and profit from the use of personally identifiable information (PII) and other consumer-based data sources. Perfect transparency in the online universe would reveal good and bad players in advance of any information exchange between the consumer and the online entity. Perfect stewardship would mean that the online entity assumes a fiduciary role or responsibility in the management and protection of PII and other consumer-based data sources entrusted to them.[2]

The following matrix provides a simple illustration of the relationship between privacy protections under high and low conditions of transparency and stewardship for online entities. The illustration shows four different conditions for information exchange between a consumer and organization vis-à-vis the Internet. It shows that the optimal conditions occur when transparency and stewardship for the online entity are both rated high. Under this scenario, consumers come to trust the online entity by virtue of its good actions, and access is therefore not needed to ensure privacy protection. In sharp contrast, when transparency and stewardship are both rated low, online entities cannot be relied upon to protect consumer privacy.

Transparency

Stewardship	High	Low
High	✓ Access is not relevant ✓ Security is implied by the actions of the online entity	✓ Reasonable access is important ✓ Security is implied by the actions of the online entity
Low	✓ "Buyer beware" ✓ Consumers understand the privacy risk and match this risk with their individual preferences	✓ Full access is necessary ✓ Data protection can not be assumed nor trusted ✓ Independent verification is essential

[2] The basic proposition is that an online entity collecting and maintaining consumer information either directly or indirectly serves as a custodian to that information in much the same way that a bank is the custodian of funds deposited by a customer.

Obviously, real life is more complex than a two-by-two matrix can show. However, the implication of this analysis is clear. That is, the key to new privacy regulation is motivating online entities to devise ways to demonstrate and ensure trust. Beyond the concept of substantial access, transparency for an online entity can be achieved through notification (with independent verification) and disclosure. While technology-based security is always a vital element for privacy, stewardship also requires the online entity to establish a culture of rigorous internal compliance.

Second, The Committee debated the issue of online access from a number of competing perspectives, reaching the following general conclusions:

- Access is important because it moves online entities in the direction of transparency.
- Full or substantial access for many online entities provides a significant cost burden that might diminish or stymie market growth.
- Access may create additional, unforeseen privacy and security risks for consumers.
- Modifying access with terms like “reasonable” creates the opportunity for regulatory loopholes and marketplace confusion, thereby diminishing its importance for the public.

As noted in the analysis above, proper notification of privacy practices may be a reasonable alternative to substantial access under conditions of trust. The notification option depends on the quality of disclosure and, most importantly, the integrity of the information source. In short, consumers alone may not be able to judge the veracity of claims made by online entities in their disclosure about privacy and security.

Independent verification or “audit” by a reputable third party is a practical solution for determining the quality and integrity of disclosure by an online entity. Independent audits of the collection, control and dissemination of personally identifiable information and other related data sources can enhance transparency, especially under conditions where substantial or full access would be infeasible for the online entity. For auditing to work as an effective agent, however, it will be necessary to first develop standards and certification requirements for auditors in this new domain of professional practice. In addition, it will be necessary to establish oversight and enforcement requirements by a self-regulatory or government body to ensure consistency, accuracy and objectivity of the auditing role.

In conclusion, the comments contained in this letter reflect my personal views and not the opinion of the firm PricewaterhouseCoopers, LLP. Again, thank you for giving me the opportunity to serve the Federal Trade Commission of the United States in this advisory role.

May 11, 2000

Statement of Arthur B. Sackler
Vice President – Law and Public Policy
Time Warner

I would like to echo so many of my colleagues in saying that it has been a pleasure and a privilege serving on the Advisory Committee on Online Access and Security. The expertise amassed around our table could not have been more impressive. The Commission deserves to be commended not only for the thoughtful, experienced individuals it enticed onto the Committee, but for the balance and diversity of points of view and backgrounds it was able to build into the Committee's composition. I would also like to give a special tip of the hat to David Medine and his crew for being evenhanded, diligent and retaining a sense of humor in the face of some fierce debates.

The report the Committee produced contains a wealth of information and options. While we were largely and, frankly, not surprisingly, unable to generate consensus on recommendations, the report has much to offer. In a sense, it is a reference work on the two vital privacy issues we studied: access and security. In this sense, it provides in one place a compendium of data and viewpoints gathered and worked through to a point.

Having said that, I would like to emphasize two related matters from the report. First, an original parameter of the Commission for the report was that access should be reasonable. Like other rights and responsibilities in our country, access should be subject to some checks and balances. Consumers as a general rule should be able to see and correct, if necessary, personally identifiable information that has been collected from or otherwise assembled about them online. But that ability should not be granted in a vacuum; it must be balanced against other needs and in light of the circumstances that apply.

Second, one of those circumstances is the harm that could be caused by failing to provide or inadequately providing access to PII. The harm that could be done to an individual's privacy from inaccuracy, mishandling and the like of personal health, financial or other such data is obvious and severe. But the harm caused by some of those same factors for less sensitive subjects is not as obvious and less severe. That difference should impact how access is applied.

Finally, I'd like to join Ron Plesser in noting that the report does not take sufficiently into account the "strides in self-regulation" that have been made over the past few short years, or the need to ensure the continued phenomenal growth of the Internet and the benefits it is bringing to consumers everywhere.

Once again, it has been a rewarding experience to have been a member of this Committee, and I greatly appreciate having had the opportunity.

Statement of Andrew Shen

Policy Analyst
Electronic Privacy Information Center

Over the past few months, I have appreciated the opportunity to attend meetings of the Advisory Committee and to dialogue with my fellow Committee members and Federal Trade Commission officials. Privacy, particularly the two components of privacy protection discussed in the report – access and security, is the foremost issue facing electronic commerce and deserves the rigorous discussion it received.

The recommendations and options set out in the report represent an impressive amount of consensus given the wide breadth of backgrounds and opinions of the Advisory Committee members. The consensus recommendation on security reflects common ground shared by all members of the Committee. While there was no consensus on access, the production of four practical options from forty-two different viewpoints demonstrates some mutual support for the different access implementation options. I myself support the total access option – consumers should have the unrestricted ability to access all their personal information held by businesses. Allowing individuals to view and control their personal information has been a basic component of privacy protection for decades and the Internet can and should provide new and easier ways for consumers to exercise this right.

If you have read the entire report, you will find that it is not dominated by technical jargon. The discussion of access largely detailed the types of personal information that consumers should be able to view and modify. It is not necessary to translate Fair Information Practices for the Internet. Moreover, we should immediately establish and enforce those Fair Information Practices for this new industry sector.

A set of legally enforceable Fair Information Practices is vital for privacy protection. Given such a system, consumers will no longer be required to pore through vague privacy policies and hope that companies are following these statements. The establishment of such a standard will also provide more direction to companies in how to design their information systems, i.e. how to "build in" privacy. Most importantly, such a legal standard will protect the basic privacy rights of American consumers. Support for legally enforceable Fair Information Practices from the Federal Trade Commission and Congress will allow us to move past some of the privacy invasions that have plagued these early years of e-commerce. There is no substitute for clear principles and strong independent enforcement of privacy guidelines.

We are fortunate in that people before us developed the solid theoretical framework of privacy protection, Fair Information Practices. With legal enforcement of these elements of privacy protection, consumers' personal information will be well protected at a level that will foster the continued growth of electronic commerce.

Now is the time to move forward to ensure that we do not pay for the benefits of new technology with the loss of our personal privacy.

Individual Statement
of
Frank Torres
Consumers Union

Consumers Union appreciated the opportunity to participate in the Advisory Committee for Online Access and Security. In the midst of the euphoria about the Internet, a few simple, yet fundamental concepts have emerged. Consumers care about keeping their personal information private, they are concerned that too much information is being collected about them, and they are troubled by how their information could be used. Often, consumers may not even be aware about intrusions on their privacy.

The work of the Committee focused on two elements -- access and security -- of what are known as "Fair Information Practices." The other elements include notice and consent. Taken together, the Fair Information Practices form a baseline for strong privacy protections. Implementation of Fair Information Practices will help spur greater consumer confidence in web-based businesses.

Access to personal data is a vital part of protecting consumers in the online environment, especially where that information is used, or could be used, to make decisions about a consumer, for example in financial or medical settings. In those cases it is also important that consumers be given the opportunity not only to see that information, but also to correct any mistakes.

Consumers need some certainty in what to expect in the online world in areas like privacy. Unfortunately, when left to the devices of the business no widespread, meaningful and reliable online privacy program has emerged. It is therefore appropriate for Congress and the regulators to enact fair and reasonable privacy rules. Far from impeding the progress of Internet such work will foster consumer confidence and help online transactions grow.

The thoughtful and detailed work of the Committee will undoubtedly be used by many as discussions about online privacy moves ahead. The Commission should be commended for seeking input from such a broad and diverse group of individuals and organizations.

Statement of Ted Wham, Excite@Home

It has been my honor and pleasure to serve as a member of the Federal Trade Commission's Advisory Committee on Online Access and Security, or "ACOAS." In concluding my responsibilities under this appointment, I respectfully submit this statement on the Committee's final Report transmitted today to the FTC. ACOAS was charged with advising the FTC regarding how domestic commercial Web sites could provide "reasonable" access to, and "adequate" security of, personal information collected online. My comments below represent my perspective, and that of Excite@Home, on an appropriate course of action to meet these objectives.

Determining what constitutes "reasonable" access to consumers' personal information involves two inquiries. First, what do consumers reasonably expect regarding access to personal information collected online? Second, what level of access can online businesses reasonably provide? Presumably, the place where consumer expectations and business realities intersect will yield a "reasonable" level of access. To be sure, both parties have a substantial interest in reaching that point. Online businesses do not want current or potential customers to forego participating in the online community because they fear losing control of their personal information. Similarly, online consumers do not want online businesses hobbled in their attempts to provide the products and services consumers demand because of overly burdensome access requirements. Therefore, any policy of reasonable access must balance the public policy objectives of providing transparent access against the consumer harm that would result from erecting undue barriers to the personalization of Internet content, or by effectively foreclosing the economic relationships that have sustained the provision of free and diverse Internet content.[3]

Bearing the interests of consumers and online businesses in mind, I, on behalf of Excite@Home,[4] would like to voice support for a proper balance of the principles underlying the Default to Consumer Access and the Case-by-Case approaches set forth in the Committee's Report.

Combining the underlying principles of the Default to Access and Case-by-Case approaches yields an access option that properly reflects consumers' expectations. The Default to Access approach requires businesses to provide individuals access to their personal information to the extent that information is retained and retrievable in the ordinary course of business. By setting a baseline presumption in favor of access, the approach matches consumers' expectations that they can access personal information collected about them. At the same time, the very provision limiting access to only that information retrieved or retrievable in the ordinary course of business protects consumer privacy by obviating the need for businesses to aggregate data in ways they otherwise would not have in order to comply with the access requirement. In a departure from the Default to Access approach, the Case-by-

---

[3] For instance, Excite@Home finds that customers who take advantage of personalized services, such as local weather or personalized stock portfolios, return to the site six times more frequently than those who do not. Similarly, the wild success of a company called LifeMinders, which provides customers with targeted "reminders" based upon their customers' provision of personalized information, dramatically illustrates the benefits many consumers perceive in providing information about themselves in return for personalized services. Based on the information gathered at registration, LifeMinders sends personalized email messages to users reminding them of important dates (such as birthdays and anniversaries), and recurring events (such as when to pay taxes). The benefits that consumers receive from LifeMinders' free service has prompted 500,000 new members to sign up – per week.

[4] Excite@Home is a portal web site which serves as gateway through which millions of users access the World Wide Web. Excite@Home provides a home base for its users by allowing them to personalize the site with news, sports scores, stock quotes, and other items of interest, and offers highly sought-after services such as email, chat, and instant messaging at absolutely no charge. Excite@Home operates the fifth largest network of Internet sites in the world.

Case approach considers a variety of factors in making the access determination, including industry sector, type of data at issue, entity holding the data, and the likely use of the information. This option properly respects the reasonable expectations of consumers by reflecting their belief that restrictions on the maintenance and use of some types of data may be more important than others.

While a combination of the Default to Access and Case-by-Case approaches appropriately reflect consumer expectations, the limitations built into their principles address the level of access online businesses can reasonably provide. The Default to Access approach limits the presumption of disclosure where it would violate the privacy of another individual, compromise the proprietary nature of certain information, or in the rare instance where the cost of providing access would place an "unreasonable burden" on the Web site. The Case-by-Case approach accommodates the proper belief that information such as health and financial data is particularly important to individuals, and is thus deserving of a greater level of access. In that way, it allows business to focus its efforts on data that is of the most importance to consumers and that, if inaccurate or improperly used, would pose the greatest threat to personal privacy.

Although the Default to Access approach gives some consideration to the level of access a business can reasonably provide, it may unnecessarily limit the ability of business to properly weigh the costs of access against corresponding consumer benefits. By limiting the cost-benefit analysis to rare instances where disclosure would place an "unreasonable burden" on the website, the Default to Access approach in practice will require the provision of access to every piece of data that flows in the course of normal Internet interaction. Consideration should be given to the value this truly provides consumers. For instance, is the fact that a customer just visited ten specific pages on a shopping comparison website something that is deserving of categorical access to that very consumer? Shouldn't the answer to this question – that would literally entail the investment of hundreds of millions or even billions of dollars to make such universal access possible across the industry – be informed by a cost-benefit analysis? It is Excite@Home's position that an "unreasonable burden" test sets too high a standard for a business to justify limits on access where the consumer's interest in the information is unclear or uncompelling. The Case-by-Case approach equalizes this imbalance by providing a more viable opportunity for business to address the critical issue of costs.

The balance between consumers' interest in access and the associated costs is reflected in nearly every iteration of the Fair Information Practices, each of which provides an exception to the access requirement for information that is not sensitive, not used to make decisions that will significantly affect an individual, not readily available, or is expensive to provide.[5] While the definition of what constitutes "sensitive" information or a "significant" decision is subjective in nature, in the vast majority of cases the appropriate classification will be quite clear. Indeed, Excite@Home emphatically supports the provision of full and complete access to sensitive data such as financial information, health information, information relating to children, and other data that – if inaccurate – would affect consumers in a materially adverse

---

[5] The 1980 OECD Guidelines, which set forth the Fair Information Practices, make clear that the right of an individual to access and challenge personal data is not absolute. Explanatory Memorandum at 17. Along the same lines, the National Information Infrastructure Task Force ("NII") has recognized that the extent to which access is provided depends on various factors, including the "seriousness of the consequences to the individual of using the personal information." See NII Privacy Principles, ¶ 30. Most recently, even the Safe Harbors drafted by the Department of Commerce to guide U.S. businesses in establishing privacy protections that meet the stringent European standards provide an exemption to the access requirement where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy. Department of Commerce Safe Harbors, March, 2000 ("DOC Safe Harbors"). In each of these examples, the appropriate threshold was deemed to be substantially below the "unreasonable burden" test proposed for the "Default to Access" approach in the ACOAS Report.

way, a touchstone of a sector-specific approach.[6] We believe that considering the issues of cost and relative consumer benefit will permit online businesses to focus their efforts on providing complete and timely access to the most critical information consumers entrust to online businesses.

Excite@Home therefore believes that a combination of the Default to Access and Case-by-Case approaches provides an adequately nuanced view of the choices that businesses and consumers must face in providing and expecting access to data. Beyond this core point, two additional implications of this view affect issues in need of further clarification:

1. Deletion of Personal Information. The Report provides some discussion of consumers' ability to delete information they provide. However, this discussion does not account for the difficulty and expense associated with "deleting" information from routine computer backup and disaster-recovery systems. Given this omission, businesses would be required to change current data storage and safeguarding techniques to comply with the requirement, or incur the costs associated with finding and deleting information from multiple systems spanning multiple locations.[7] For that reason, consumers should be provided the opportunity to delete all consumer-contributed information only where deletion is easily accomplished under the information holder's data storage practices. Where erasure of this information would pose undue administrative burdens or substantial costs, the company should be instead required to deactivate the consumer's account. Information associated with inactive accounts could then be deleted consistent with the company's standard data retention business practices.[8]

2. Access to Inferred and Derived Data. Consumers should not have access to inferred data (defined as information gathered from sample data that is calculated to result in a value that is applied to the data subject) and derived data (defined as information gathered from the data subject that is calculated to result in a value that is applied to the data subject). Inferred and derived data can only be generated though the application of proprietary business processes such as algorithms, terminology, and classifications unique to the company's marketing inferences or other business decisions. Providing consumers access to inferred or derived data may impinge the company's right to make private decisions regarding who to target for marketing purposes. Identical decisions are made hundreds of times per day in the offline environment with no analogous opportunity for access.[9] Exempting inferred and derived data from access

---

[6] Existing U.S. privacy laws reflect an industry-by-industry approach to information privacy based upon the sensitivity of the data and its intended use. As the Report indicates, individuals have the ability to access and correct financial and medical information as well as information used to make employment decisions.

[7] The purpose of backup and disaster-recovery systems is to provide a means for recovery of data that is lost due to acts malicious or accidental. For instance, it is only prudent for businesses in earthquake-prone Silicon Valley to store copies of their critical business information, including consumer data, in locations physically separated from their main course of business – having multiple copies of the data, present in multiple locations, is the whole idea. Backup systems especially do not lend themselves to easy record-by-record deletion, nor does the continuing presence of consumer data on a historical backup tape that may have been deleted from the counterpart online system entail a significant privacy risk.

[8] Most online businesses have reasonable lengths of time after which even inactive or disabled accounts and their associated data are purged.

[9] For instance, no customer in the offline environment could reasonably expect a retailer to provide access to the information they used in deciding to send that customer a certain catalog or discount offer.

obligations would comport with the most recent iteration of the Fair Information Practices which exempt from the access requirement "confidential commercial information," which includes "marketing inferences or classifications generated by the organization."[10]

In closing, it is my belief, and the position of Excite@Home, that combining the principles underlying the Default to Consumer Access and the Case-by-Case approaches will enable online businesses to hone their efforts and best serve their customers by providing extensive access to the most desired data.

My thanks are given to the Federal Trade Commission for the opportunity to participate in the important work of the Advisory Committee on Online Access and Security. I will also take this opportunity to thank my colleagues, the other members of the ACOAS, who were able to engage in a lively but professional discourse intended to illuminate these difficult issues. While a very broad spectrum of opinions were offered, each member of the Committee strived to ensure that all opinions would be reflected in the final Report, and I believe they are. I have the greatest respect for the selfless nature of the work done by these colleagues and am proud to be identified with the fruits of the Committee's collective efforts.

Ted Wham
Excite@Home
May 15, 2000

[10] See, e.g., DOC Safe Harbors, Draft Frequently Asked Questions No. 8, March 2000.