

Testimony of

Hans Peter Brøndmo

Author, *The Eng@ged Customer: The New Rules of
Internet Direct Marketing*

Netcentives, Inc. Fellow

Before the

Senate Commerce Committee on

Internet Privacy

Wednesday, July 11, 2001

Chairman Hollings, Senator McCain and Members of the Committee thank you for inviting me to participate at this important hearing on Internet privacy. My name is Hans Peter Brøndmo and I am a technology entrepreneur, author and consultant to industry on the usage of customer information and email to build customer relationships. I believe that these hearings are timely because we find ourselves at a fork in the road where one path can lead us to a win both for individual rights and for industry, while the other takes us down a treacherous path where all parties loose. Strong leadership and decisive action will ensure that we choose the correct path.

At the center of the debate about Internet and privacy is a simple question: Who owns information about an individual? Does each person have rights to and control of the information being gathered about him or her or should whoever collects the information be able to use and commercially exploit it in any manner they see fit? While the question may be simple the answers are complex.

My remarks today focus on the broader issue of information ownership in which I propose a framework for how we think about collecting and using personally identifiable information, consistent with our belief both in personal liberty and in free enterprise. I will return to this framework momentarily. First let me take a brief look at where we find ourselves at this moment in time.

Brøndmo Testimony....page 2

It seems that historically the rules which govern what information a company can collect about its customers and prospects and what they can do with this information favors industry over individual rights. For example, there have been egregious instances in which many a credit worthy individual has been summarily denied a home mortgage, auto loan or educational financing on the basis of incorrect personal data that had been surreptitiously collected and never submitted to the person for

verification. Erroneous data often has been through the hands of several firms without the individual's knowledge, making correction impossible. Meanwhile, without effective recourse, a deserving individual's personal life is severely damaged.

The attitude that dominates the current business environment is that federal privacy legislation will hamper free enterprise and limit industry's ability to grow and innovate. I disagree with this attitude and believe that we need to move away from the mindset that any information a company captures about their customers is theirs to exploit and even sell in whatever manner they see fit. I would like to propose that industry allows the free market to determine the value of their integrity. If customers trust the organizations they do business with and these businesses have integrity, customers will award them with access to their personal information. If not, it seems only reasonable that a customer must be allowed to inspect or withdraw that information. An obvious question is why now? If we have managed so far, why can we not continue on the same program? And the answer is obvious – The Internet. According to what we read, every device and tool we rely on to enhance our lives will soon be connected to the Internet: our automobiles, our homes, our

Brøndmo Testimony....page 3

cellular telephones, our television sets, our hand-held cameras, our Jacuzzi tub, our electronic credit card. And while the benefits are many including pervasive access to information and the ability to communicate regardless of location, there is a dark side. These devices will pass along information about who is using them, where they are located and perhaps even details about what a person is doing. This information about individuals can be collected and analyzed in ways that were not possible prior to the Internet. The potential threats to privacy are enormous.

While the new technologies present fantastic opportunities and real threats to individual rights it is also important to recognize that the challenges posed to industry are real and formidable as well. Internet technologies are changing the manner in which companies conduct commerce. They are fundamentally impacting the way businesses communicate with and service their customers. It's a

fact that personally identifiable information is a key ingredient to individualized and successful commerce in an information economy. Just as fossil fuels powered the industrial revolution and new transportation technologies made it possible to achieve economies of scale, information is the fuel of the global economy and the Internet is the engine powering an explosive growth. My experience has convinced me that if the ability to collect and use customer information is compromised, American industry will be at a competitive disadvantage. That said, business as usual will not do.

Brøndmo Testimony....page 4

While some industry leaders are holding themselves to high standards, a majority of businesses still think in old terms regarding how to realize value from personally identifiable information. Corporations needs to come to terms with a new definition of the value they realize from such information both in order to safeguard personal liberties and in order to realize the vast potential of properly managed information.

Central to this definition of value are two assumptions: first that customer information is a precious capital asset and second, that the individual, not the company they do business with owns and controls information about themselves.

Acting on these two assumptions, let me return to the framework that I made earlier reference to. It goes without saying that no modern business survives long in today's fiercely competitive marketplace if it keeps its financial assets in disarray not knowing how much working capital is available and who has the money. Yet that's exactly how most companies manage their customer information. They don't know what they've got, they don't know who has what and they don't know what databases contain what information. It turns out that the comparison between financial capital and information capital is a good way to illustrate the new framework. Consider the following familiar example from the banking industry.

Like most Americans, I have money in the bank and I have a stock portfolio. I have chosen to hand over my financial assets to professional asset managers. I keep my money in a local bank and I work with a stockbroker. When selecting my bank and stockbroker I had two primary selection criteria: TRUST and RETURNS. If I do not trust a bank I will not give them my money. And if the competition, the bank next door, consistently offers better returns what will I do? I will withdraw my money from my current bank and deposit it with the competition.

As individuals we are increasingly becoming aware that our personal information has real value. And just as we will choose to deposit our financial assets with asset managers based on TRUST and RETURNS, we are learning to apply the same two criteria when we “deposit” our personal information with a company. And if that company breaches our trust or does not manage our information in order to generate a return in the form of good service and convenience, we will withdraw it and deposit it with a competitor who does.

Information that an organization collects about the individuals it interacts with should be treated like a capital asset. It is this information, when used properly, which enables a company to build relationships with their current and prospective customers and to realize significant financial gain from its ongoing interactions with those customers. Without access to personally identifiable information companies cannot get to know their prospects and customers. And if they cannot know and enter into a personalized dialogue

with the very people they do business with, it is equivalent to not being able to greet a customer when she walks into a store. Or even worse, not being able to develop a relationship with that customer and recognize her for her loyalty when she returns to that store over and over again.

Yet does the customer want the store to know who she is before she has introduced herself? Does walking into a store for the first time constitute implicit permission for the store to dip into a database and look up who she is? Would she be comfortable if a grocery store knew how many children she has the very first time she entered? Would she be concerned if the grocer sold their knowledge about her low-fat diet to her insurance provider without her permission and knowledge? The issue is one of personal choice about personal data. And these are the types of questions we are asking when we discuss “opt-in” policies, notice and access.

To address these important concerns, I offer four principles that exemplify the new thinking I believe must be adopted in order to realize the potential value and benefits inherent in the smart use of customer information.

- Organizations (data vendors) represent themselves as the custodians – not owners, of personal information
- Organizations invest in and actively manage the information they gather about individuals in order to generate a return to those individuals as well as to all other constituents (shareholders)

Brøndmo Testimony....page 7

- The individual owns and controls his or her personal information and chooses to deposit it with a company based on expectations of TRUST and RETURNS.
- Individuals receive many benefits such as better service and more relevant information, timesavings and achieve higher efficiencies as an organization gets to know them by collecting and appropriately utilizing personal information about them.

While the argument that industry self regulation can address all these principles may seem appealing, it is my belief that unless we have uniform and consistent rules providing a foundation

for these principles the individual cannot rely on for protection and consistency. Furthermore it means we do not have a level playing field for industry.

Let me share with you an example that illustrates some common misconceptions and hurdles that confront those who favor giving customers proper notice, access and control of their personal information. And while this example illustrates a company that did the right thing in the end, it also illustrates that doing right by the customer is doing right by the business and therefore that appropriately written legislation will have a net positive impact on business.

The email marketing company I founded in 1996 has worked for several years with an online music retailer. Some time ago the retailer was experiencing a customer satisfaction problem because they were sending too many promotional emails to their customers. Once you had made a purchase from the company you were added to their marketing

Brøndmo Testimony...page 8

database and began receiving electronic commercials. It was very difficult to stop the flood. We argued for better notice and a simple and straightforward unsubscribe mechanism, making it easy for customers to remove their name from the mailing list. The company hesitated to heed our advice for seemingly logical reasons: They had spent tens of millions of dollars on marketing to attract their customers and we were telling them that if a customer wanted to disengage, it should not only be possible, it should be easy. They could not convince themselves that “letting a customer go” was good business. As their satisfaction problems continued to grow the music retailer finally decided to perform a test with a small sub-segment of their customers. They implemented a very simple one-click unsubscribe process for the test-customers making it easy for them to stop the emails or modify their personal profile. To the retailer’s great surprise, they discovered that their new process had no negative impact on the business whatsoever. The people that complained about receiving too many emails were not likely to make any more purchases. More astonishing was the fact that when the company rolled out the new functionality to their

whole customer base and promoted on their e-commerce web-site how easy it was to opt-out, their level of opt-in improved significantly. People were more comfortable signing up when they knew they were in control and it would be easy to disengage from the service should they not want it in the future. Providing customers with the ability to easily access and change their personal profile information, including removing their names altogether built trust and confidence. The music retailer profited from making it easy for its customers to unsubscribe or disengage.

Brøndmo Testimony....page 9

As this example illustrates determining what is appropriate notice and what represents adequate permission in order to collect personally identifiable information is not simple. Furthermore it would also seem that there is no single solution appropriate for all situations. My experience has convinced me that opt-out with notice may be an appropriate level of protection in many instances. Yet there are also many cases where strict opt-in is the only appropriate solution. In situations where information is being collected strictly for internal use in an organization, my opinion is that an appropriate level of protection is afforded by requiring opt-out with notice. Where there may be possibilities that personally identifiable information will be transferred to an external organization that an individual is interacting with, it seems the only appropriate solution is to require full opt-in.

What is key here is the concept that no matter the circumstance, every firm must assume full responsibility for protecting personal data entrusted to it, whether by customers, employees or prospects. Implementation will necessarily vary with circumstances but as in matters of law, policies will indicate intent.

Finally we must acknowledge the considerable cost to industry implicit in requiring stricter enforcement of notice, permission and complete access to and control of personal information. In my opinion the requirement that industry provides individuals with access to and control of personally identifiable information will be the most costly component to implement as it probably requires that such information be centralized.

Most organizations do not have the technical ability to centralize their customer information today, nor do they have the internal processes to enforce uniform and appropriate use of customer information. That said, it is feasible to implement such solutions with existing technology and developing best practices business processes to support such an initiative is a question of good management. Furthermore, the policy changes an organization must undertake to implement proper privacy protection for its members and customers are the same initiatives essential to focusing the organization around its customers, an important trend in business and marketing. In other words, the investment made to protect the individuals' privacy, is an investment in best business practices and will generate handsome returns when made a corporate priority.

America is a country of innovators and inventors. The way personally identifiable information is managed by industry must change and I am convinced that the spirit of innovation and creativity will lead us to new and significantly enhanced solutions. I have no doubt we can create options that support industry's need to collect, combine and even share personally identifiable information, all without compromising individual privacy.

In order to drive this change, I believe that government regulation is necessary. While it is not the role of government to dictate to companies what they may do with customer information, it is the responsibility of the federal government as an extension of its constitutional duty to protect civil liberties to ensure that the use of information is based on the consent and always under the control of the individuals to whom it belongs. We

need a foundation for major change as well as a level playing field and only federal legislation can establish the required ground rules. While industry self-regulation can work in some cases and in some states, it will not be an effective way to ensure that a win-win scenario for the all citizens of

America and for industry alike. When it comes to protecting privacy and empowering a competitive data industry, the federal government, in my opinion, has an indispensable role to play.

Mr. Chairman, and Members of this Committee I am encouraged by your leadership in this area and thank you for the opportunity to address the committee this morning.