Understanding business consortium approaches to privacy: What does the Customer Profile Exchange Specification truly mean for personal privacy?

JoEllen Osburn

Follow this and additional works at: http://scholarworks.rit.edu/theses

Recommended Citation

This Thesis is brought to you for free and open access by the Thesis/Dissertation Collections at RIT Scholar Works. It has been accepted for inclusion in Theses by an authorized administrator of RIT Scholar Works. For more information, please contact ritscholarworks@rit.edu.
Understanding Business Consortium Approaches to Privacy

What does the Customer Profile Exchange Specification truly mean for personal privacy?

Revision 1

Submitted by:
JoEllen Osburn

MS IT concentration areas:
Information Technology Strategy
Software Development and Management
Student Name: JoEllen Osburn

Thesis Title: Understanding Business Consortium Approaches to Privacy

What does the Customer Profile Exchange Specification truly mean for personal privacy?

Thesis Committee

<table>
<thead>
<tr>
<th>Name</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edward Holden</td>
<td></td>
<td>5/8/2002</td>
</tr>
<tr>
<td>Chair</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.A. Lawson</td>
<td></td>
<td>5/8/2002</td>
</tr>
<tr>
<td>Committee Member</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Larry Hill</td>
<td></td>
<td>5/8/2002</td>
</tr>
<tr>
<td>Committee Member</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Understanding Business Consortium Approaches to Privacy

What does the Customer Profile Exchange Specification truly mean for personal privacy?

I, JoEllen L. Osburn, hereby grant permission to the Wallace Library of the Rochester Institute of Technology to reproduce my thesis in whole or in part. Any reproduction must not be for commercial use or profit.
Introduction ........................................................................................................................................... 3

Why do businesses feel that they need initiatives such as CPEX? ..................................................... 5

The CPEX Specification .......................................................................................................................... 13
  What does it promise to do and how does it plan to do it? .................................................................. 13
  What does it attempt to collect? ........................................................................................................... 17
  What are the inherent problems with CPEX's approach to data collection? ................................... 20

How will the Platform for Privacy Preferences Project influence CPEX? ......................................... 26
  What does the Platform for Privacy Preferences Project do to promote privacy? ......................... 26
  What doesn't the P3P specification do? .............................................................................................. 29
  Can the public really expect any protection from the CPEX or P3P standards? ............................ 33

How does CPEX explain the lapses in privacy protection in relation to its standard? .... 37

What does the future hold? .................................................................................................................... 39

Conclusion ............................................................................................................................................. 42

References ................................................................................................................................................ 45
"The right to be left alone---the most comprehensive of rights, and the right most valued by a free people."
Justice Louis Brandeis, Olmstead v. U.S. (1928) (Hodges, 1)

Introduction

As the Internet steadily becomes a more ubiquitous part of our lives, it is enabling data collection techniques that are capable of creating detailed consumer profile databases that link both on-line and off-line consumer behavior data without the individual's knowledge or consent about what is being collected or how it is being used. This has been seen as troubling as it seems to infringe on individual privacy for the sole sake of corporate profit. This infringement has been an increasing cause for concern since business consortiums have recently banded together to make the gathering and sharing of private, personally identifiable information even easier through the use of industry-wide data collection and dissemination standards. As a result of this consortium effort, privacy, as it relates to Internet transactions and a business's self-assumed right to collect unlimited amounts of data regarding them, has come under greater government scrutiny and may result in greater governmental regulation of such transactions. Business consortiums, however, state that no such concern on the part of government agencies is necessary as the profile exchange methodologies that they are
developing will not only allow them to share data more effectively and efficiently, thus allowing them to reduce their costs, but, they argue, will also allow them to ensure that personal privacy is maintained. This, in turn, will empower the consumer and negate the need for government regulation.

One consortium project that maintains that industry self-regulation is best suited for protecting individual privacy, and that is at the forefront of the movement for profile exchange standardization, is the Customer Profile Exchange (CPEX) group. The CPEX project purports itself to be a “vendor-neutral, open standard for facilitating the privacy-enabled interchange of customer information across disparate enterprise applications and systems (Cover)”. It furthermore states that its goal is to “enable enterprises to implement the privacy safeguards their customers and governments require in a unified approach, rather than piecemeal in each application (Cover)”. With such simply and overtly stated goals, it would be easy to assume that perhaps CPEX could meet the needs of both business and individuals, and therefore truly offset the need for government oversight regarding privacy regulation and administration. However, it has often been said that a chain is only as strong as its weakest link, and this is proven to be abundantly true when discussing the CPEX initiative from the individual’s point of view rather than the business’s point of view as has typically been done. When this is done, one finds that the standard proposed by the CPEX group is riddled with privacy-eroding factors that mitigate its ability to protect anyone’s privacy and that actually serves only to bolster the strength and influence of large, multi-national corporations at the individual’s expense. This is true in both the development of the specification itself, the privacy-enabling specifications on which it builds, and with the methods currently used by businesses to supposedly enforce privacy protections using industry initiatives alone. Until these mitigating factors are effectively removed from all aspects that the
standard involves, government involvement will be absolutely necessary to maintain any semblance of privacy at all.

Why do businesses feel that they need initiatives such as CPEX?

Before the Customer Profile Exchange standard and its accompanying ramifications can be understood, one must first understand why there is a perceived need for such a specification to begin with. The reasons all stem from the increasing globalization of business concerns and their accompanying pursuit of increased profits. Stated most simply and directly, businesses exist not for the public good, but to make a profit. The amount of profit to be made is directly related to the amount of product that can be sold. The more product that can be sold, the greater the profitability for the company. One of the best ways to sell more product is to inform more potential customers that a given product is available and convince them to buy it via any means possible. Direct marketing campaigns such as targeted mail campaigns, telemarketing, and targeted banner ads on the internet have all shown themselves to be very effective means of doing this, even though the response to any given campaign can be relatively low (i.e. a response rate of less than five percent is typically interpreted as being a very good response rate). This type of behavior then is very beneficial for businesses as it allows them to expand their spheres of influence at minimal costs.

Even though direct marketing has shown itself to be profitable for American corporations, there are still basic rules that businesses must follow in carrying out initiatives that involve such types of customer interaction. Expansion marketing is fine, but must be cost-efficient and profitable as well. For this reason, business entities try to
match their offerings with people that they feel will be most likely to purchase their products. For example, they don't want to try to sell a Lamborghini to a family that lives on a poverty level income as this type of marketing initiative would not be an effective nor efficient use of advertising budgets as the targeted household would not be able to purchase the product being promoted. In instances such as this, the business, literally speaking, would be throwing its advertising budget away as uses such as this would not bring additional revenue to the company. Therefore, in order to prevent this type of scenario from occurring on a frequent basis, businesses must of course collect and analyze personally identifiable information to prevent potential customers from getting inappropriate marketing materials.

The information that is gathered typically falls into three major categories. The first category is known as geographic information, or where one lives, and is comprised primarily of address data, and the quality of the address data (i.e. what census tract the that address is in, latitude, longitude, and geocoding information which is used to perform tasks such as drive-time analysis or trade area analysis about how far a person will travel to shop at a particular store). The second major category is perhaps the most familiar to us and is known as demographic information. The information in this category consists of information such as name, address, phone number, marital status, and reported and modeled information such as a person's income level, whether or not residents of a particular address have a propensity to purchase via mail order or on-line, are home owners or renters, and whether or not they are credit card users. Generally speaking, this information is used to gain an understanding of what an individual person or household is really like. The third category of information generally collected for making marketing decisions is called psychographic information. This information shows marketers what the subjects of the target market are really like in terms of their behaviors as it describes the life-style indicators. These life-style indicators tell
marketers whether the subject is an avid reader, gardener, hobbyist, cyclist, etc, and thus allows companies to further hone their marketing potential in regards to contacting potential clients that would most likely be interested in their products. This information is often compiled from lists and surveys and is aggregated by some collection of relevant factors that varies from request to request (United States, 7).

All combined, these three types of data allow marketers to perform complex modeling and analysis processes that can be used to determine which households might, and just as importantly, might not be interested in, or most likely can or cannot afford a particular product. All of this serves to help businesses get the highest return on their marketing expenditures by ensuring to the highest degree possible that their marketing materials are sent to those potential customers who are most likely to buy the pitched products.

There are several key concepts in this process that drive businesses towards data collection and toward data collection standards like CPEX. First, and most obviously, if businesses are to pursue direct marketing in an efficient and cost-effective manner, they must have an adequate store of data to work with. This means that they will naturally be driven to collect as much geographic, demographic, and psychographic information as possible to understand the potential customer base in terms of its interests and its propensity to buy particular products. Perhaps not so obvious at first glance, however, is the purity of the data in the data store. As mentioned in the discussion involving the types of data available, much of it is self-reported, collated from surveys, or aggregated by third party data collectors. The majority of this data is correct and very accurate, and, taken collectively, gives a fairly accurate picture of the purchasing habits and behaviors of the targeted household. However, depending on the data source, this same data can also be very generalized, or even very inaccurate, depending on the "honesty" of those that are being surreptitiously profiled.
This imperfect knowledge can have negative impacts on a businesses profitability. By this, industry leaders mean to say that though they can determine which products are selling, they cannot always determine who is buying them, or what complimentary purchases they might be making or convinced to make through the use of the proper marketing channels. This inability to determine who the precise target market is thus deprives businesses of revenue as they cannot use their marketing activities in an effective and efficient manner to attract and retain new customers. Surely the key to being able to do this is being able to collect the desired data from potential customers on a real-time basis, directly from the consumer himself. If this can be done, the data obtained will be as close to 100% pure and accurate as is humanly possible.

As one can imagine, being able to use data such as this effectively not only makes the corporation extremely profitable, but also extremely powerful. With it, companies will be able to tune their marketing activities so that they perfectly match the potential customer by pitching the “right” product at precisely the “right” time. This increased marketing savvy will, in turn, allow the corporation to maximize its profitability, strength, and flexibility on a global scale. This, in turn, will lead to even greater desires to collect and use ever greater amounts of personally identifiable information. The companies that do this most effectively will, for all intents and purposes, “own” their customers economically as they will find themselves better and better able to meet their needs, so much so that the business’s competitors may be effectively eliminated.

Therefore, one could say that increased access to such pure information will truly become the most valuable currency of the marketplace. Indeed, it can easily be said that in today’s society, “the principal measure of our wealth is information: its quality, its quantity, and the speed with which we acquire it and adapt to it (Brook, 29)”. Already many Internet-based companies are reporting that their very profitability comes from
their ability to collect, use, and sell consumer data as they see fit, regardless of what they had previously promised customers.

As a result of this mentality, it is easy to see how the information as a source of wealth principle works in the "real world" by examining both Amazon's use of data and Toysmart's bankruptcy case. Amazon, easily the most well-known of the Internet's book merchants, has for some time collected and used personally identifiable information to its advantage. Indeed, the company has not yet made a profit, but continues to be one of the highest selling Internet stocks because of the information it has and what it has done with it. The company is continually refining this data and attempting to use it in new ways designed to increase the company's profit margin. Indeed, in early 2001 the company found itself the focus of negative attention because of the manner in which it used information to offer the same product to different consumers at different prices. Though Amazon denies it, this was done in an effort to determine the price-sensitivity of different consumers. Clearly, Amazon was using the information in its database in an attempt to gain greater profits by charging select customers higher prices.

In the Toysmart case, the major focus of the discussion was over Toysmart's willingness to directly contradict its privacy policy by transferring its personally identifiable information regarding its customers to a third party. While this is of great concern, perhaps of even more concern in terms of this specific discussion is the fact that Toysmart realized the value of its data and attempted to use it as a bargaining chip to enhance its own financial coffers when it was filing for bankruptcy protection. Indeed, Toysmart listed not just its customer list as one of its assets, but also offered for sale its database of personal information including names, addresses, and buying habits in an attempt to recoup some of the losses it suffered (Rosencrance, 2). Indeed, part of Toysmart's dilemma was caused by the fact that it deliberately used this data as an attempt to gain as much cash as possible, turning down offers from Digital Research...
(which had offered $15,000 for the data) and Disney (which had offered $50,000) saying that the offers were too low (Rosencrance, Disney, 1), even though Toysmart had promised its customers that it would never give, rent, or otherwise share its data with a third party. Though Toysmart did finally accept the offer from Disney, this case is still an excellent example of using information as a source of wealth and power.

A specification such as that represented by the Customer Profile Exchange project that can actually deliver the data necessary to meet increasing information demands on a real-time basis would, of course, be of extreme interest to any corporation seeking greater control over its profitability, its customers, and perhaps its competitors as well.

That being said, the current state of business marketing intelligence must also be examined in order to further understand why businesses need data collection and dissemination standards such as that proposed by CPEX. There are two basic problems in this area that businesses need to overcome to make their marketing initiatives as profitable and economical as possible. Those problems are efficient data use and economically sustainable customer acquisition costs.

Collecting the data needed to make crucial marketing decisions is one thing; being able to organize it and use it to provide maximum profitability is entirely another matter, and is one which businesses claim they have not yet been able to master. This is because businesses claim that customer data within a single corporation alone often lies in multiple, disparate databases. This disorder and lack of integration renders the data nearly useless for coordinated business activities such as targeted marketing campaigns and customer retention activities such as enterprise resource planning, customer relationship management, and intelligence analytics to work together. Each of these systems typically has its own way of representing customer data and integrating these disparate systems efficiently and meaningfully is often an arduous, if not nearly
impossible task. Having a single, well-coordinated database from which to draw on for all of these activities would allow the company to use this data to effectively serve both marketing and customer maintenance and retention purposes. This single view would, therefore, allow businesses to provide more value to their customers, thus increasing the company's bottom line in tangible, financial areas and also in the intangible areas that include items such as customer good will. If the customer felt that doing business with the business was very easy because the company could assist with the current situation and perhaps anticipate what the customer may need in the future, he would be more prone to return to that business for his future needs as he would be assured of obtaining fast and efficient service. The end result of this process would, of course, be increased revenue flows for the business as it could effectively determine what the customer wanted and needed before the customer actually perceived these wants and needs himself.

Having this unified view would additionally allow businesses to save time and money on integrating enterprise solutions. This is a problem currently faced by all market segments that is only bound to get worse as the prevailing data collection, merging, and analysis landscape becomes ever more complex and sophisticated. This is especially true where companies seek to expand such a singular customer view outside of their own corporate walls and use it to profitably interact with other companies, each of which has its own disparate system of databases. Without a unified view of the customer, businesses will find themselves spending ever increasing amounts of time and money attempting to understand their customer's desires and how to meet them. The CPEX specification would greatly reduce these costs through the use of its standardized data collection and dissemination components. This is important because the need for a unified view of a customer is critical for business success according to 90% of companies interviewed by Forrester Research, but only two percent of those businesses
claim to have it in place already. Among those expressing a desire to have such a system, few have little idea how to get there (Fisher, 2). CPEX aims to help such businesses make the necessary connections to overcome this obstacle in as efficient and economical manner as possible.

Lack of a unified view of the customer additionally increases customer acquisition costs as more money must be expended by the business entity in order to attract a sufficient quantity of interest to actually result in income for the company. This is especially true in the Internet world. Marketing strategies typically in place there are very inefficient and result in the expenditure of vast sums of money to attract each potential customer. For example, if company A purchased 133,000 banner ads, and paid around $15 per thousand for those ads, it would probably earn around 300 or so visits from those ads. Of those visits, it would be expected that only five would take any action whatsoever on the site. Of those 5, only 20%, or 1 customer, from the initial 300 that had been attracted by the ad would truly be expected to make an additional purchase within the next year. This results in projected acquisition costs of $2,000 per customer (United States, 35) for businesses relying on Internet advertising to increase their profitability. Clearly, the market as a whole cannot view this as being an acceptable amount to spend per customer in terms of acquisition fees. The market clearly needs to be more focused on how it attracts and retains its customers. According to industry intelligence, only a standardization specification such as that put forward by the CPEX group can hope to reduce these costs to acceptable limits, and thus preserve the Internet as a viable marketplace for both buyers and sellers. These economies of scale will be possible through the data sharing capabilities offered by the CPEX specification. As the profile is exchanged between member companies, it grows ever richer as a result of the additional data that it accumulates at each rotation. This allows business to continually refine its target market criteria at the least cost possible.
The CPEX Specification

*What does it promise to do and how does it plan to do it?*

Billed as being the first global standard for privacy-enabled customer data interchange, the Customer profile Exchange standard has rather lofty aims that it states in simple, straight-forward language. By its own definition, the CPEX specification seeks to create a “vendor-neutral, open standard for exchanging privacy-enabled customer information across different businesses and computer systems” that will “apply to Customer Relationship Management (CRM), customer care, the Internet, back office applications, front office applications, application servers, networking, supply chains – anything that touches a customer (CPExchange, 1)” The immediate benefit of using this system is to enrich corporate coffers by bringing them the Holy Grail that they have long sought - a single, holistic customer profile that will allow them to market their products perfectly in terms of reaching maximum profitability levels. This may be accomplished via two different methods. The first and most obvious method will be made possible by allowing participating companies to directly target the “correct” consumers for one’s products. The second and lesser known manner is by allowing participating companies to forge new strategic alliances with one another through data sharing efforts, thus bolstering the profits of both organizations.

Just as important, as facilitating the collection and formatting of the data, at least according to the group’s 1999 press releases, is maintaining consumer privacy. In fact, several press releases relating to the launch of the project make repeated references to this feature of the specification. An article appearing on ZDNet stated that “while a major component of CPEX is the standard method for sharing data, the real key to the effort is
privacy. CPEX developers want to find a way to give consumers a means of controlling information about themselves at a fairly granular level (Kerstetter, 2). An article appearing in The Register further reinforced this idea as it stated that "the scheme itself actually includes provisions for the responsible sharing of information, such as enabling one company to make data available only to others that agree to similar use restrictions, and enabling consumers to access and even control their data profiles while confronting a single, consistent format (Greene, 1). These statements were not just the result of overly hopeful or confident members of the news media. They were, in fact, echoed by Brad Husick, one of the key players in the development of the CPEX specification. When questioned about CPEX’s ability to protect customer data while at the same time fostering greater data collection and sharing efforts among member business entities, Husick stated "The key for CPEX will be to make it as easy as possible to apply whatever privacy policies do emerge. Our intention is to be a privacy advocate and to make the privacy community aware and involved in the effort (Duvall, 1). This was important, he said, not only for doing business in the American business arena, but for conducting it on a global level as well.

As might be expected in today’s technological world of object oriented programming and use of modular code, the CPEX standard seeks to "reuse and interoperate with existing work, rather than to reinvent (Dumbill, 1). Using elements such as this allow the specification to develop to maturity at a quicker rate as it uses proven techniques where possible and thus allows the entire specification to be developed at less cost and ostensibly with a greater degree of reliability and effectiveness. Under the project’s plan these goals would be met by a three-pronged approach that would consist of three major components. The first component is a data model for collecting customer information (to be XML based to allow all specification participants to share a single data format that is easily understood by both technical and
non-technical people alike. This would ensure that all applications using the specification, whether internally or externally, spoke the same "language "and used the same terms"). The second component planned for the specification is a privacy model to be compliant with and built upon the Platform for Privacy Preferences specification. The third component is a transport architecture for query and data interchange purposes." (Dumbill, 1). These collective processes would make analysis tasks quicker and easier to perform as the data would already be in the correct, known format when it arrived at the company that desired to analyze it. The participating company would merely have to apply its own set of analytical tools to the data to determine how to use it to gain competitive advantage.

As a result of these goals, according to specification developers, business entities and their customers would both be better served. As has already been mentioned, businesses get the single, holistic-view customer profile that they have been seeking. Customers, on the other hand, ostensibly get ensured data privacy protection and better service from the companies they do business with as a result of the greater "personalization" benefits that participating companies will be able to offer as a result of the data repository features offered by the specification. The result of this specification at this point in time seemed to be a win-win, dream-come-true scenario for all participants.

As a result of this combination of benefits, the specification quickly gained a stellar group of over 70 participants that easily represent some of the largest American companies in nearly every market segment. Among its members, CPEX counts financial giant First Union, technology giant International Business Machines (IBM), Internet advertising giant DoubleClick, and privacy rights specialist Zero Knowledge Systems. This combination of companies endowed the specification with great credibility and prestige. CPEX's founders, its members, and members of the trade press all envisioned
great benefits for businesses and customers alike because of the combination of companies that the specification had been able to attract. It was often noted that even companies that seemed to be bitter rivals or at opposite ends of the political spectrum (such as DoubleClick, well known for its attempts to gain access to as much personally identifiable knowledge as possible, and Zero Knowledge systems, well known for its attempts to thwart entities such as DoubleClick) had joined the specification effort. If this was the case, it was concluded, the specification must be headed in the right direction as conventional wisdom would not have thought that companies that were bitter rivals or at opposite ends of the political spectrum would unite in sponsorship of a specification that would harm themselves or their business reputations.

This, however, is where the dream ends and the reality of business consortium efforts to control data privacy begin to appear. Simply stated, CPEX's publicly stated vision and the reality that it is creating are two entirely different and, for the most part, totally irreconcilable entities. Privacy, it will be shown, has been sacrificed on the ever-hungry altar of corporate greed. This can clearly be shown by analyzing the data that the specification hopes to collect and how it has fared in its stated goal of ensuring privacy for the data that it collects.
What does it attempt to collect?

One of the key features of the CPEX standard is its data collection facilities. Before getting into the specifics of the information to be collected, it is important to understand the significance of the data that is collected. All data to be collected by this specification comes directly from the potential customer himself and is gathered via surveys and forms the consumer fills out online as well as from website interactions that the data subject participates in. Unlike information that is culled from third party databases, there is no aggregate data present in the database on a default basis, though CPEX members may choose to receive it in aggregate form if they so desire. All of the data is personally identifiable and gleaned directly from the subject, in many cases without him knowing about it and without his permission. Its purity, for all intents and purposes, is as close to being 100% as is humanly possible. This is because the specification effectively acts as a tracking device and voraciously picks up every bit of personally identifiable information that it can find. This is ostensibly all done in the name of better personalization for the customer. No longer will businesses be able to say that they do not have enough facts to judge where their marketing budgets should be spent to achieve the most desirable results. The CPEX collection methodology is, indeed, every marketer's dream come true. This can be seen by examining some of the types of data that members of the consortium hope to collect.

The breadth and depth of the information that this specification seeks on potential consumers is unmatched in current schemes. Examination of the specification reveals that it is designed to pick up nearly all information that can be used to define an individual, much of which individuals consider to be extremely private and highly confidential. All combined, this information is a complete dossier on the individual's life as it is designed, in part, to be an historical record of his transactions and activities. At a
basic level, it seeks to know name, contact information (including postal address, e-mail address, telephone number, fax number, pager, cell phone number, and website), primary residence, social security number, nationality, taxation identification number, passport number, citizenship status, residency status, preferred language, and best days and times for initiating contact. It then delves into demographic data that it defines as being "general characteristics" that are widely applicable to business processes, personalization, and market targeting. This includes information such as gender, birth date, education, income level, race, number of dependents, maiden name, marital status, date of marriage, spouses name, whether or not the person is a smoker, etc. The specification also contains what it terms "activity information" which consists of personal information such as one's employment status, employer, length of employment, job title, base pay, frequency of pay, annual bonus pay, percentage of person's total work time spent in the occupation, and hobbies. The specification extends its intrusive data collection abilities even more by making it possible to record an individual's financial data such as type of bank account, account number, and credit cards owned and their corresponding numbers (though it does make a miniscule attempt to preserve privacy here by not incorporating balance or transaction information for this type of data). This information can additionally be linked with a person's web site interaction data such as site visited, specific pages visited, content viewed, etc. This combination of demographic and behavior activity combined with the ability to actually track a person's movements in real time gives the business entity an unprecedented ability to observe the customer in his natural habitat, thus providing the data collector with knowledge about the consumer that heretofore was unavailable, and all of which may be kept as long as the collector wishes to keep it and used however the data collector or his self-selected associates choose to use it.
It is imperative to note that the data gathering specification is not finished at this point in time and, in reality, may never actually be finished since the object model that represents the data to be collected will be “enhanced as experience and continued work identifies additional cross-industry profile information that would be desirable to have. In particular, a representation of a household with relationships between members of the household and their roles in the household could be useful in many industries (Bohrer, 88)”.

This is troublesome because it seeks to profile all members of a household without their permission and regardless of their age, for unknown purposes. Work is being done even now to ensure that industry groups can extend the specification as desired when desired, even if there is no specifically defined purpose regarding how the additional information that is collected will truly be used or if there is any obvious legitimate or beneficial business purpose for the data at the time it is collected.

This information promises to be a veritable treasure trove to consortium members that choose to use it. Seeing that it has all of these data elements together in one place, its users will be able to accomplish feats that were not possible before. Consortium members will be able to track almost every move a customer makes (i.e. what does he look at, for how long, how many comparisons does he make, what does he actually purchase). This is important data to have as it has already been proven that past behavior is the single greatest predictor of future behavior. Heretofore, this knowledge has not existed for internet purchases. The CPEX specification would change that and allow its members to see this data in real time, across different marketing channels. Targeting customers will be much easier with the data advantages promised by the CPEX initiative as there will truly be no place for consumers to hide their most personal information or behavioral habits and no enforceable limits as to how consortium members can use it.
What are the inherent problems with CPEX’s approach to data collection?

Though the CPEX initiative’s approach is potentially a wonderful boon for commercial entities, the same cannot be said about its impact on personal privacy rights as there are several inherent problems with the data collection approach that the CPEX specification seeks to implement. Among those problems are undefined data necessity which leads to information bloat with no clearly defined benefit or reason for collection, the potential to use the specification to circumvent current privacy law through the use of new data sharing agreements, and inadequate data protection via the specification itself. All of these issues render the specification incompatible with fair information practices as defined by the Organization for Cooperative Economic Development (OECD) which attempts to harmonize data transfer activities between member nations such that all parties are treated equally and fairly and that international trade can proceed as freely and responsibly as possible. If the CPEX specification cannot remedy these problems, its members will likely find themselves severely restricted in their abilities to traffic in international data currencies as the OECD seeks to minimize hazards in this area by restricting data flow to rogue entities that have little or no regard for personal privacy. Therefore, the efforts CPEX is making to maximize corporate profits by exploiting consumers for information that can be used to generate information capital may actually find that its efforts actually accomplish the exact opposite.

First of all, the data is collected on an indiscriminate basis, with provisions already being made to expand the amount and type of personally identifiable data to be collected. This goes counter to generally accepted practices for privacy and data sharing advocated by the OECD which state that “privacy protection starts with the initial collection of the information to ensure there is a good reason for doing so and only for
legitimate uses for which, where necessary, the individual has given an informed consent (Modernising, 1)”. The factors represented by this statement are a collective representation of the following OECD data collection principles which are designed to protect individual privacy and promote legitimate business needs for personal data:

1. Collection limitation principle. This principle states that consumers must have knowledge of and give consent to collection practices and that there should be practical limits to the amount of data collected.

2. Data quality principle. This principle states that data must be relevant for the purposes for which it has been collected, and is accurate, complete, and up to date.

3. Purpose specification principle. This principle states that the purposes for which personal data is collected should be specified not later than the time of its collection and its subsequent use limited to the fulfillment of those purposes.

(Guidelines, 4).

The CPEX specification is not able to meet these definitions at this point in time, and in fact, is not likely to do so at any point in time in the foreseeable future either. This is due to the fact that CPEX reserves the right to expand its data collection practices at any point in time and that there are no mechanisms in place at any level as required by OECD policies to ensure that consortium members adhere to any sort of fair information collection and use practices.

This will handicap the specification in the future as it goes against what is currently happening on a world-wide basis in the industrialized world in regards to concepts regarding the collection and use of personally identifiable information as well. The European Union (EU), whose member countries, like the United States, are members of the OECD, has already passed data privacy laws that prevent CPEX’s data
collection mentality from being the prevailing manner of doing business in its member countries. Under its privacy laws, the data collector must get the expressed permission of the data subject to collect the information and can use it only for the purpose for which it was collected. Thus, businesses in these environments must clearly show why they need to collect the data as individual privacy is valued as being more important than a businesses desire to collect such information and profit from it via any means possible. It is important to note that EU members are legally bound to honor those commitments. Participation in them is not voluntary as it is under CPEX. Other countries, such as Canada which is also one of the United States' major trading partners, are rapidly following the European lead and building personal privacy provisions into their laws as well. Practices such as these clearly show a legal concern for personal privacy as it is at the forefront of the decision making process in regards to data collection in all but the United States.

In the United States, however, we are starting to see a grass routes campaign for personal privacy policies springing up in some of the larger companies that are more attuned to the current atmosphere regarding public perceptions of privacy and business infringements upon it and how failing to incorporate personal privacy initiatives may actually harm the business's profitability. Many companies are starting to hire Corporate Privacy Officers (CPOs) that actively seek to become "data minimalists" rather than "data maximalists" as advocated by the CPEX consortium. One of the most successful of these is Wal-Mart. Wal-Mart has used its inventory and forecasting technologies to become perhaps the world's foremost and most profitable retailer. Most of its initiatives, shockingly enough, have come without requiring vast amounts of personally identifiable information. Clearly, having access to unlimited stores of personally identifiable information is not the only key to profitability as some consortium members have advocated. In fact, some companies are beginning to realize that following data
maximization principles will actually result in the attraction and retention of fewer customers because of fear of privacy infringement. As a result of this, CPEX must get into the habit of asking itself "why is the data being collected needed"? and work only with data that is absolutely necessary. Only by doing this can it ensure that the data it collects is used properly and not exploitatively and that personal privacy is maintained. Clearly, CPEX cannot afford to take unrestrained and unlimited data collection for granted if it wishes to succeed either with business entities or with consumers in any part of the world as powerful business entities in the United States and other parts of the world are already moving away from its methodologies and towards policies that ensure greater privacy for individual citizens.

There is also growing concern that the "new strategic alliances" that this specification would allow companies to forge based on the large amounts of data collected and the ease with which it could be exchanged would negate existing privacy protection laws. If this ability is left unchallenged, the propensity of CPEX to encourage such endeavors will greatly diminish personal privacy as there will truly be no controls, voluntary or otherwise, that can adequately protect sensitive, private data. This method of circumventing existing privacy law may in fact, result in human rights violations through inappropriate data uses that harm individuals. This ability can be illustrated by examining the Graham, Leach, Bliley (GLB) Act and analyzing CPEX's potential impacts on its effectiveness.

The GLB act provides overarching privacy protections for consumers relating to their relationships with financial service institutions. GLB was drafted mainly to allow financial institutions, insurance businesses, and investment institutions to merge and combine services, with the proviso that they maintain the privacy and security of any non-public information relating to their customers. Therefore, under the GLB Act, financial institutions must provide all customers with privacy notifications stating exactly
what information is collected, how it is used, and with whom it is shared. Additionally, all financial institutions must allow customers to opt-out of any third party data sharing efforts with non-affiliated entities. This is an iterative process that must be completed each year to maintain compliance with the law. This Act, then, shows considerable concern about the collection and use of personally identifiable information and seeks to give consumers as much explicit control over it as possible.

There is concern, however, that the CPEX initiative and the loose associations that it allows business entities to form in order to gain competitive advantages through greater knowledge of personal behaviors would allow financial service companies to circumvent the privacy protections mandated under GLB by conducting any desired data collection or exchange programs under the auspices of the CPEX specification. Senator Richard Shelby has already questioned CPEX's possible infringement on the effectiveness of the GLB act in many areas. He questions, for example, whether a financial entity such as First Union would be able to circumvent GLB protections by becoming a member of the CPEX consortium and exchanging information with other CPEX members who are not financial institutions, and therefore not required to abide by GLB's non-public personal information control standards (Shelby, 2). This type of activity could allow financial institutions to continue to surreptitiously engage in the exchange of private personally identifiable information without disclosing its use or allowing customers to opt out of it as required by GLB. They may not even have to disclose that they share information with companies such as MicroStrategy or DoubleClick whose sole purpose is to sell individual customer data for a profit. It is very conceivable that this could be done as section 6802 of GLB states that financial institutions cannot share data with non-affiliated third parties. Through membership in the CPEX consortium, however, and the strategic alliances that companies under its shelter will be able to forge, financial companies will conceivably be able to claim that
the alliance with the third party is indeed affiliated with the company itself. It could, therefore, skirt GLB’s consumer privacy protection laws and freely share information that it would not be at liberty to share otherwise. Shelby additionally speculates that under conditions such as this, CPEX membership may also inhibit the ability of an audit process to accurately verify whether or not an institution under the jurisdiction of GLB was in fact operating within the constraints of the law or used its CPEX affiliation to circumvent it. As of this point in time, Senator Shelby’s concerns have not been addressed, thus, the negative repercussions they address have not been mitigated under the CPEX standard. Under these less than certain operational methods, it is very conceivable that this murky network could compromise non-public information that the Graham-Leach-Bliley Act was intended to protect. CPEX can, therefore, be seen as an erosive agent in regards to personal privacy in this area.

This apparent ease of circumvention and the privacy erosion that it allows again goes counter to OECD concepts of fair information use regarding data banks and use of the data contained in them. The OECD clearly states that “countries have a common interest in preventing the creation of locations where national regulations on data processing can easily be circumvented; indeed, in view of the international mobility of people, goods, and commercial and scientific activities, commonly accepted practices with regard to the processing of data may be advantageous even where no transborder data traffic is directly involved (Guidelines, 8)” Clearly, laws will be needed to prevent businesses from using circuitous avenues such as that exposed by Senator Shelby regarding the financial industry from negating the few privacy protections that are currently operating in the United States. Allowing consortiums such as CPEX to remain in control of such areas will only result in greater dissolution of personal privacy at an ever increasing rate.
How will the Platform for Privacy Preferences Project influence CPEX?

There are then many proven instances and conditions under which the CPEX specification has been shown to be a privacy-erosive standard rather than a privacy-enhancing one as it claims to be. Privacy advocates can easily prove themselves to be defenders of the public good by exposing the weaknesses of the data collection portion of the specification alone. To its critics, however, the CPEX consortium would say that it has mitigated the risks just discussed by interfacing its specification with the Platform for Privacy Preferences specification. To be sure, this specification does offer some protections, but it, like the CPEX specification itself, is severely lacking in its ability to provide adequate privacy protection for the data gathered under the auspices of the CPEX specification itself. This can be more clearly understood by examining what the P3P specification does and does not do.

What does the Platform for Privacy Preferences Project do to promote privacy?

A cursory glance at the CPEX technical specification is at first shocking when one considers the depth and breadth of the information that the specification proposes to make available to consortium members. Then, one discovers the privacy declarations that are also part of the specification. At first glance, these have the potential to make one believe that, given all of the shortcomings in the data collection methodology, the data is still secure as it is protected by a privacy declaration, just as promised by the consortium's initial press releases. Indeed, a cursory examination of this portion of the CPEX specification sounds like a dream come true for the consumer who wishes to shop.
and browse without fear that data will be collected and used against his wishes and without his knowledge.

In fact, the information contained in the privacy declaration seems to be very protective of individual rights as a whole, so much so that one may even believe that government intervention is not necessary. According to the CPEX specification, the privacy declaration segment of the process contains information such as "specific policy characteristics that describe how data can be used, how long data can be retained, and whether access may be granted to the individual's data, and for what purposes (Bohrer, 27)." It is even possible to assign different privacy levels to different aspects of a particular profile, ostensibly to provide more protection to more sensitive data. As a result of this, one begins to think that the CPEX specification truly can meet the needs of both business entities and individuals without the need for government intervention. This is reinforced by the fact that all of these privacy principles are reinforced and advocated by the OECD. All of these protections are, however, as is specifically stated in the CPEX specification, directly dependent on the technical underpinnings of the Platform for Privacy Preferences project and as such are not directly part of the CPEX specification itself. It is at this point that CPEX begins to distance itself from the policies related to privacy as the specification repeatedly points out that the P3P specification is responsible for much of the privacy protections that the CPEX specification states that it encompasses.

This is not all negative, however. In deed, there are many positive aspects to the P3P specification that truly make it worth consideration. It does, for example, promote the OECD concept of the use of privacy policy statements that are easy for both humans and machines to understand and interpret. In fact, it is the expressed purpose of this specification to collect information from consumers regarding their privacy expectations for the expressed purpose of matching them with the particulars involved in a web site's
posted privacy policy. If any discrepancies are found between the user's expected privacy level and the site's privacy level, the P3P user is notified of the discrepancies and is then free to choose whether or not to interact with the site or proceed with a transaction. This is very important as the Federal Trade Commission has recently been regarding a web-site's posted privacy statement as a legally enforceable document, and having the data in a standard, machine interpretable language can prevent the user from having to read every privacy statement for every page he or she visits and try to interpret it correctly. If the specification itself can retrieve this data, interpret it, and rely on it to be correct, the consumer can make very well informed decisions about matters pertaining to his or her privacy and feel relatively confident that his privacy desires are being maintained.

The specification seems to be forward-looking as well as it takes into account that business entities may change their privacy policies at any point in time. For this reason, the specification suggests that privacy policies have expiration dates which it checks periodically to determine whether or not the site's privacy principles are still in agreement with the consumer's preferences. In this manner, consumers will be able to maintain on-going control of how much personally relevant information is released about them and to whom it is released.
What doesn’t the P3P specification do?

There are however, unfavorable aspects of the P3P specification that render it unreliable in terms of being able to completely mitigate the privacy concerns that arise from the CPEX specification. Some of those deficiencies require one to delve into the specification’s inner workings to unveil P3P’s shortcomings; others, however are discernable by simply reading the specifications overtly stated purpose.

Upon close examination, there are many areas in the P3P specification that should be cause for alarm when attempting to understand its treatment of personally identifiable data and how it can be used to give data collected and exchanged through CPEX the additional protection that is required according to CPEX’s own publicly made statements regarding privacy’s place in the consortium’s efforts. Among the most pressing concerns here are the facts that whether P3P is set up correctly or not to “protect” the data subject properly, users may be “forced” into using lower privacy settings via one means or another, that the specification is inoperable with jurisdictions that require strong privacy standards, that it firmly shifts the onus on privacy protection to the user rather than the data collector, and that it cannot be relied upon to ensure that web sites implement and use it correctly or reliably as it has no legal enforcement specifications.

The P3P specification relies on extremely specific language that is meant to guide the user through setting up his or her own privacy profile. This may be a daunting task to some users that ultimately results in them giving themselves very few privacy rights, not because they do not want them, but because they do not understand how to configure the software properly. Such inexperienced users may even depend on the use of default privacy settings supplied by browser manufacturers such as Microsoft and Netscape. This will be detrimental to individual privacy as these entities rely on
advertising to supplement their profitability and as such will deliberately set privacy protection standards lower than the average user might like in an attempt to maximize profits.

At the other end of the user experience and understanding spectrum, however, may be those that do understand the specification and its associated ramifications and that, therefore, set their privacy protections higher. These users may find that by granting themselves “too much” privacy, as defined by P3P enabled web-sites, they are inundated with pop-up windows warning about privacy infringements. These interruptions may occur so often that they truly prevent the system from being workable in a P3P user’s daily interactions on the Internet. This may become so burdensome that users turn the privacy protection settings down, just to avoid the inconveniences associated with the pop-up windows. It is even conceivable that users with high privacy settings will be effectively blocked from viewing site content at all due to incompatible privacy preferences set by the web site itself, and thus will be “coaxed” into lowering settings just to view content. This behavior will, of course, tip the data privacy scales firmly in the direction of the business entity, with the end result being that the individual has no more privacy or control over his data as a result of P3P and CPEX than he did before either specification had been conceived. Of course, in instances such as this, business will claim that the consumer has the amount of privacy he required without mentioning how it happened that the consumer suddenly determined that less privacy was needed. Therefore, rather than being a privacy-enhancing technology, P3P may in point of fact become yet another privacy-eroding technology.

This, and the fact that the P3P specification was not designed to be an enforcement mechanism, greatly limits the specification’s applicability in jurisdictions where strict privacy enforcement rules exist and thus dilutes the privacy protections that the CPEX initiative is attempting to offer members, regardless of where they or their data
subjects are located geographically. For example, P3P has no ability to ensure that sites follow their posted privacy policies nor that data is not exchanged when the user’s privacy policy and the web site’s policy do not match. All it can do is determine what the user wishes to have in terms of privacy and what the site says it offers. There is absolutely no verification process going on between any of the entities involved in any given transaction involving P3P. This violates the OECD concepts of fair information use in terms of enforceable limitations and audits and renders the P3P specification unusable for large segments of the Internet using community.

The European Union (EU) is an extremely good example of this. EU member countries demand that privacy infringements be dealt with strictly and that they be legally enforceable. As the P3P specification does not do this, the EU has expressly rejected the P3P specification from being part of its privacy framework. This is both because the standard seeks out lowest common denominator approaches to privacy and because of the EU’s belief that:

"a technical platform for privacy protection will not, in itself, be sufficient to protect privacy on the web. It must be applied within the context of a framework of enforceable data protection rules, which provide a minimum and non-negotiable level of privacy protection for all individuals. Use of P3P in the absence of such a framework risks shifting the onus primarily onto the individual user to protect himself, a development that would undermine the internationally established principle that it is the data controller who is responsible for complying with data protection principles (Pretty, 6)"

This shortcoming alone negates P3P’s ability to adequately implement privacy for the CPEX standard. This is important because the CPEX consortium is actively courting the members of the European Union in hopes of getting business interests from those regions to join the specification. Weak protections such as that provided by P3P may make that goal impossible to meet as they clearly dilute privacy protection practices.

Overall, there is little evidence to persuade one that P3P actually has much power to truly protect the data that it is supposedly given jurisdiction over. This is,
surprisingly enough, abundantly apparent merely by reading the project's technical specifications. Unlike the CPEX specification and its relationship to privacy, the Platform for Privacy Preferences project is, in many areas, very up-front and clear about what it does not do. The specification clearly states that "although P3P provides a technical mechanism for ensuring that users can be informed about privacy policies before the release of personal information, it does not provide a technical mechanism for making sure sites act according to their policies (Marchiori, 6)."

The specification further states that companies using it may provide assistance in this area, but are not required to do so under P3P guidelines. This is a very clear statement to any company that utilizes P3P as part of its privacy strategy that P3P provides no enforcement methodology for actually protecting data privacy. As it provides no enforcement mechanism, as is required for OECD-compliant information use practices, it cannot truly protect the privacy of any data it is associated with as users of the specification can freely circumvent its intended purposes with impunity. It is additionally important to note that the P3P specification does not protect privacy so much as it "aids" consumers in terms of negotiating how much privacy to give up — and even that part of the process cannot be counted on to occur reliably as there are no enforcement mechanisms or punishments for those business entities that refuse to play the game fairly. As has been said, this is stated rather bluntly on the P3P web site. One does not have to go on a hunting expedition to find this information or read between the lines to interpret what the specification is saying. It firmly spells out in plain black and white that it does not actively protect data privacy.

This, of course, would have been immediately and unequivocally known to CPEX’s designers and can only be interpreted as being a gaping hole in information protection policies that CPEX was aware of and totally negligent in correcting. In fact, it can even be said that CPEX used the P3P specification to deliberately mislead the
public regarding the privacy protections that it, and in turn CPEX, truly offered. Basically, the P3P specification asks all of its participants to play nice and not break the rules. This is not something that anyone should depend on happening on a strictly volunteer basis.

**Can the public really expect any protection from the CPEX or P3P standards?**

The use of P3P for protecting data gathered and shared under the auspices of the CPEX project, therefore, is just as problematic as the data collection problems that the CPEX specification chooses not to remedy. This is both because the P3P standard was not meant to actually perform any sort of enforcement and because CPEX knowingly incorporated this specification within its own with no attempt whatsoever to provide the data protection facilities that it knew the P3P specification did not have. P3P, like all current American developed products of this sort, is a voluntary specification, and even within the CPEX specification itself, its use is considered to be optional. That is to say that there is no requirement whatsoever within the CPEX specification itself that mandates that privacy control information of any kind be placed on any data at all. Companies have free-will over whether or not to participate in the P3P standard, and even how honest they want to be if they do participate. This is critical because P3P can truly only work if it is widely available and if companies that use it do so responsibly and honor the expressed wishes of consumers. Therefore, CPEX’s claim to grant individuals privacy regarding the data that it collects should be regarded as being tenuous at best. It is, in fact, using P3P to give consumers a false sense of privacy and security as neither CPEX nor P3P has any real power to ensure control
over privacy or security from either the consumer's or the business's standpoint. This is because the CPEX initiative relies totally on voluntary participation and practices at both levels of its specification where any relevant privacy protection measures could be invoked.

There are already several indications that the P3P specification will not be honored on a voluntary basis, even by members of the CPEX consortium itself. As has been shown earlier, the CPEX standard is saying "We're going to collect the data and you're invited to the party" (Rupley, 1). This is abundantly proven by the specifications continual search for yet more personally identifiable information. The first question one should ask here is "Who's party is it?" The answer, of course, is that it's business's party, not consumers' and business is reserving both the right to collect any data it wants and the right to use it in any way it sees fit. Tellingly, though there are preparations for privacy data to be included, they are not mandatory as part of the CPEX specification itself. This speaks volumes about the true function of privacy as a whole as it relates to CPEX's true end goals in serving the needs of consumers and individuals. As a result of the specification's willingness to relegate true privacy implementation to a third party and its reluctance to even state that the third party specification must be used for all data associated with the CPEX specification, the average consumer can expect precious little protection in terms of privacy when it is in the hands of self-regulation activists such as the CPEX consortium.

At a Federal Trade Commission conference held in March, 2001 to discuss the topic of data collection merges and exchanges and at which CPEX representatives were in attendance, Ted Wham, President of Database Marketing for the Internet whose career has been concentrated in the direct and database marketing industries summed up the feelings of many marketing specialists when he said "I fundamentally reject the notion that a consumer should be able to say I want to do business with a particular
company Y, but that company can't follow on and make money out of that relationship. I think this has terribly negative consequences for the efficiency of economic transactions in this country" (United States, 30). Yet another participant, Jerry Cerasale, Vice President for Government Affairs at the Direct Marketing Association, echoed Wham's feelings in the following statement which was made at the same conference: "I try and sell you, provide you with these radios at the lowest price possible. I hold down costs as much as possible. In that light, I share and rent your information to others and provide the savings on to you. I do not provide you the opportunity to not participate in this sharing. I do not provide access opportunity (for the customer to review the data that is collected and disseminated to other parties, another key factor of the OECD guidelines concerning fair information practices) to you because both of those things will increase my costs and therefore increase the cost of my goods to you. If you don't like this, please, please shop somewhere else (United States, 64)"). One’s first reaction to these statements might be, “but they are only the opinions of two men. You can hardly judge an entire industry by the comments of one or two individuals”. Sadly, while others are not as vocal as Mr. Wham or Mr. Carasale, they do seem to share their sentiments. In fact, fully 61% of corporations polled in a recent study conducted by Zona Research indicated no interest in the P3P specification specifically, and more than half of them also stated that they had “no intention” of joining any privacy consortium whatsoever (Jones, 1). What Wham and others like him are truly saying is that, regardless of what the consumer indicates he wants, business is going to pursue the avenue that brings it the most revenue, privacy be damned. Clearly, voluntary standards such as those espoused by the Platform for Privacy Preferences and the CPEX specification will not truly be able to protect individual privacy to any measurable degree by working on a strictly volunteer basis.
How does CPEX explain the lapses in privacy protection in relation to its standard?

It is interesting to look at the CPEX initiative one year after its initial debut. Whereas in its 1999 press releases CPEX continually stressed the importance of maintaining privacy, the very word itself now seems to have been nearly erased from the project’s vocabulary. Indeed, Brad Husick’s statements regarding CPEX which once focused on the privacy angle now state that “CPExchange (CPEX) doesn’t guarantee enforcement. …The point of the standard is to make data storage easier for individual companies.” He continued with “…wouldn’t it be great if when you call the customer relations department, about a problem with a new laptop you bought, that they knew exactly what kind of machine you bought and when you bought it” That’s what the standard does. It helps with the customer service. (Jacobus, 3).” Privacy, as one can see, no longer seems to be a critical part of the project, nor a point upon which the overall success of the project will be judged.

As a recent study by the Cutter Consortium pointed out, “privacy has to do with whether you can collect certain information. Once you’ve collected it, privacy is a moot point (Cutter, 1)” This statement is certainly representative of the CPEX consortium’s approach to the privacy problem, and is indeed one that can easily be demonstrated by examining the CPEX specification itself. Such an examination reveals very enlightening information about the role of individual privacy in regards to the project’s specification overall. According to its technical specification, CPEX “established the following requirements on its specification:

1. Platform/application/vendor independence
2. Communications protocol independence
3. Market acceptability
4. Message envelope independence

5. Operation independence"

(Source: Bohrer, 13)

Marketing acceptance, as can readily be seen is number three on the list. Individual privacy did not even make it to the list, though it had previously been touted as being extremely important. This relative unimportance of privacy to the specification is made strikingly clear in the schematic the group shows in the published form of its specification that shows the specification's major categories and their interrelationships. The link between the system's core data and its privacy protection layer is shown as being entirely optional. This shows that the idea of privacy is far from sacrosanct in CPEX's view. This is yet another tell-tale sign that the specification should not be taken seriously in its claims to protect individual privacy at all. The customer, as one can see, is completely left out of the picture now, except as a source of exploitation for the enrichment of the corporation.

Sure, CPEX promised to protect privacy, but, as can now be shown, it had no actual intention of doing this directly or even indirectly in any type of manner that could be regarded as being reliable and trustworthy. Instead, it treats privacy as an afterthought to be looked after by someone else. CPEX, after all, wants the cache associated with being a privacy advocate as that perception is sure to help its member organizations increase their revenue streams, but does not want to take responsibility for enforcing it. It is, therefore, derelict in its responsibilities to the consumer. The CPEX specification, is then, extremely negligent in its treatment of privacy and should not be looked upon as being capable of self-regulation or above the need for governmental privacy regulation.
What does the future hold?

It is tempting to find fault with these findings regarding the apparent inappropriateness of the business consortium approach to privacy. Admittedly, this can even be relatively easy, depending on one's political and personal beliefs. Regardless of those beliefs (i.e. whether or not one is an ardent believer in the right to personal privacy or whether or not one believes that the marketplace will protect the privacy rights of individuals adequately without external intervention), it must be recognized that there will always be some legitimate need to collect personally identifiable information. It can also be successfully argued that the majority of companies would use such data in a relatively reliable and responsible fashion. This being the case then, are CPEX's shortcomings something that the American public, as a whole, should overlook? Has the ever more vocal privacy-advocacy minority overstated the reasons for concern? Can industry successfully police itself and circumvent the need for governmental regulation to protect the privacy of the average citizen?

There is, of course, no crystal ball that can give us the answers to these questions. As the old saying goes, "only time will tell". It is possible, however, to examine the behavior of those closest to the project and use that information to derive a very plausible answer to these questions now. Interestingly enough, if we turn the profiling tables round-a-bout for a moment, and analyze data gathered from businesses involved with the CPEX project, some rather intriguing items come to light that just might show how viable CPEX might be in the future.

DoubleClick, as might be recalled, is one of the staunchest supporters of efforts such as CPEX. CPEX does, after all, further DoubleClick's aim of gathering as much personally identifiable information as possible with as little regulation as possible and using it for corporate profit. Seeing that this is an industry wide initiative that is
supposed to be beneficial to both the business and the consumer, one would think that DoubleClick would be touting its participation in the project and would be eager to educate the public on how consortiums such as this would be most beneficial to the common consumer, and should, therefore, be supported by all for the common good. This, however, does not appear to be so. When visiting DoubleClick’s Internet site, no mention is made of the CPEX project at all. This is a bit peculiar seeing that the CPEX specification was originally intended, and touted in all of its early press releases, to be extremely protective of the disclosure and use of any personally identifiable information. DoubleClick’s behavior may be understandable given the overwhelming backlash of negative publicity that it received last year for its attempts to surreptitiously collect such information and use it for its own financial gain. Fear of another such backlash may indeed be preventing DoubleClick from forthrightly disclosing its participation in the development of the CPEX specification on its own site. This behavior might then be understood and minimized as a beacon of trouble for the initiative. However, this behavior can also be seen as a setback in terms of CPEX’s adoption and use as even its most ardent collaborators are being relatively silent about their participation in its creation and evolution.

Two other original backers of the initiative, financial industry giant First Union, and investment industry giant, Charles Schwab, both among the ranks of the very few non-vendor, yet major end-user companies involved in the project which could have served as both its first implementers and champions have seemingly backed away from the project and are eager to disavow any connection with it. While First Union merely downplays its involvement in the specification when asked about it, Charles Schwab representatives rather bluntly say that it was “just a fluke that the firm was listed as a member of CPEX; the company had joined only to pick up some XML (Extensible Markup Language) tips” (Thibodeau, 2). One really cannot distance oneself from the
specification much more vehemently or forcefully than this. Clearly affiliates that once
were enamored of CPEX's promises are now treating it as a privacy pariah and are
seeking to break any ties they may have to the initiative before their involvement in its
development becomes common knowledge and a profitability liability.

The behavior of yet other CPEX associates, though they don't seem as callously
cunning as DoubleClick or as ambivalent as First Union and Charles Schwab, leaves
little to the imagination in terms of interpreting their feelings about the CPEX initiative
and what it must have if it is to survive. Indeed, associates such as Vignette and IBM
seem to be acknowledging that the current specification has problems, and may even be
signaling that the focus of the specification must be changed once again if it is going to
survive. Brad Husick, vice president of software-maker Vignette, one of the original
organizers of the CPEX initiative, has publicly admitted that, although CPEX has a global
focus, "the group would benefit greatly from more non-US involvement," and that he was
"actively seeking more participation from the European Union (Dumbill, 1)". This is a
very clear, though veiled, admission that American business approaches to privacy,
such as that proposed by CPEX, which advocate protection through self-regulation only
will not win in the global arena. If the specification is to succeed here, it must embrace
regulation meant to ensure that companies act in a responsible manner as over forty
other countries in the world have already done.

IBM Chairman and Chief Executive Officer Lou Gerstner is even more forthright
in regards to this area, both in his public communications and in his internal IBM
communications. In an internal memo distributed to IBM employees on November 28,
2000, well after IBM had joined the CPEX bandwagon, Gerstner stated "At its core,
privacy is not a technology issue. It is a policy issue. And the policy framework that's
needed here must involve the information technology industry, the private sector in
general, and – despite what some in our industry believe – public officials." In public
communications, he echoes this, but also stresses that "the answer must begin with a responsible marketplace. Through our policies and practices, industry has to send an unambiguous message that tells people: ‘You can trust us. You have choices. They will be respected. And you’ll know in advance how any information that you give us will be used. (McGuire, 1).” These statements clearly indicate support for an approach that embraces both industry self-regulation and for legislation such as that used by the European Union. As such, they also negate CPEX’s assertion that privacy is best guarded by new technologies, not new laws.

In reality, neither of the two is a workable solution in and of itself. Only by using a combination of these two methods will Americans know any form of privacy. If CPEX is to survive, it must not only patch the loopholes that render its self-regulation approach flawed almost to the point of being unusable, it must also embrace what has thus far been its number one nemesis – industry regulation by the government.

**Conclusion**

A recent study by the International Labor Organization (ILO) identified American workers as being subject to the most intense surveillance pressure of any population of laborers that they surveyed (Brook, 37). The CPEX initiative, if left unchecked, will only intensify this pressure to the detriment of the American society as a whole as it would unfailingly give corporate America a disproportionate amount of control over the average citizen’s most dearly held basic right – the right to privacy when carrying out his or her daily activities. As has been shown, business attempts at self-regulation have been riddled with loopholes that the industry can, has, and will continue to use to effectively get around any so-called privacy initiative that it might ostensibly claim to be protecting through polices advocating self-regulation only.
Actually engaging in any such self-restraint would, in effect, cause the business involved to "leave money on the table" (Perine, 202), something that a business in search of profits is loath to do. Standards such as that proposed by CPEX make this even more problematic as it makes it perfectly clear that "If anything, the system has become more complex and companies are becoming more clever at getting around the weak protections that exist (Olsen, 3)". For all practical purposes, then, it is impossible to conclude that the CPEX standard can act as both the data collector and the privacy arbiter and perform both jobs in an effective and satisfactory manner for all parties concerned. There must be some government oversight to ensure that fair marketing practices are followed and that individual privacy is respected and enforced.

This will be absolutely mandatory if the United States is to retain control of the Information Superhighway and the E-commerce activities and revenue associated with it, and it must occur quickly. There are already over 40 countries that have legislation in place to protect individual privacy rights, with Europe having set the pace for that legislation (Melmuka, 1). Already, the European Union's advances alone threaten to leave the United States two decades behind in regards to protecting privacy (Smith, 2), which Americans have long held to be one our most basic and necessary rights. The inadequacy of our current privacy protections will not only erode personal privacy rights in the United States, but will erode the financial well being of the very companies that are fighting to keep government regulation out of the fight over privacy rights.

American businesses often speak of the money they will lose if they are not allowed to freely collect and trade any information that they desire. What we do not hear them talk about is the money they will lose in the global marketplace if they do not accept some controls over how privacy is protected. According to some published reports, billions of dollars in Internet commerce was lost last year alone, not because of insufficient knowledge of customer preferences on the part of corporations, but as a
direct result of the hesitation on the part of European consumers to purchase products from businesses that do not protect their privacy (Marer, 3). This figure can be expected to increase this year and succeeding years as a result of additional countries such as Canada that are following the EU's lead and providing more data privacy protection to their citizens. If American business entities truly wish to engage in and benefit from this most potent form of currency, they must be willing to listen, not only to the citizens of the United States, but also to those of the entire world, and ensure that personally identifiable information is collected judiciously and carefully and protected to the highest degree possible. Anything less will be to the detriment of the American corporation and its profitability, and ultimately to the detriment of the American dominance of the Internet marketplace.
References


