Aims and Scope

The Journal of e-Business and Information Technology is a semiannual international journal which aims to publish articles of high quality dealing with how online business technologies relate to the information technology, addressing various e-business forms and their evolution, and covering all aspects of IT, particularly those touching the Internet.

The intention of the Journal of e-Business and Information Technology is to help the local and global business communities to efficiently exploit IT towards the creation of business value in e-business. The journal welcomes all types of applied research studies in global computing that add value to e-business owners, customers, developers, and evaluators. That is, applied studies in IT, online business technologies (all e-business forms, e-commerce, etc.), and Internet security are particularly sought.
Journal of e-Business and Information Technology

Volume 03 Number 01, Fall 2002

From the Editor-in-Chief

E-Lending: Foundations of Financial and Consumer Marketing in an Information Intensive Society
Alan D. Smith and William T. Rupp, Robert Morris University ………….. 5

Customer Loyalty and Privacy on the Web
James P. Lawler, Pace University ..................................................20

Applications and Process Strategies of Bar Coding Technologies in the Health Care Industry
Alan D. Smith, Robert Morris University ...............................37

Right of Privacy and Advertising: United States and European Union Conflicts
Roy J. Girasa, Pace University .......................................................51
From the Editor-in-Chief

The Journal of e-Business and Information Technology is a semiannual international journal which aims to publish articles of high quality dealing with how online business technologies relate to the information technology, addressing various e-business forms and their evolution, and covering all aspects of IT, particularly those touching the Internet.

Even though most online business technologies attracted only large businesses and banks in the past, due to the high costs involved, the rapid development of the Internet made it feasible for individual consumers and small businesses to participate.

Today, every business in the global market place is certainly affected by the Internet, and business technologies on it. Popular information technologies used for online business include 1) the traditional EDI which employs private telecommunication lines and value-added networks, 2) the Internet EDI (I-EDI), and 3) electronic commerce (e-commerce). More e-business configurations are arriving every day …

Owners are however faced with the real challenge of creating business value in e-business and redefining the new requirements and directions for survival or success in this new online business environment. Owners do not hide the fact that information technology, EDI, and e-commerce have become not only necessary for success, but a fundamental requisite for survival.

It is e-business if you fail and e-business if you thrive…

With its exceptional preeminence, the Internet embraces almost the whole field of business and touches at some point or other, on almost every social issue of our time.

Let us have this forum where we all learn how to design, develop, and exploit IT to plan business value in e-business.

BelRagga

Bel Gacem Raggad, Ph.D.
Editor In-Chief
E-Lending: Foundations of Financial and Consumer Marketing in an Information Intensive Society

Alan D. Smith, smitha@robert-morris.edu
William T. Rupp, rupp@robert-morris.edu
Robert Morris University
Department of Management and Marketing
Pittsburgh, PA 15219-3099

Abstract

E-lending can significantly reduce the amount of time it takes to process loans, by allowing the potential borrower to do much of the work. The cost savings for presumably many thousands of applications per year will be substantial. However, the start-up costs for e-lending can be significant. Lenders must be confident of volume projections. E-lending provides another opportunity to gain wallet share. Thus, offering e-lending services to your already savvy Internet customers allows banks to increase the amount of business with that customer. Lenders can use the increased flow of information and real-time interaction to offer a variety of products and services that are relevant to a particular customer. E-lending also allows lenders to reach borrowers outside of their traditional market areas. In malls, the customer can do research on products, rates, terms, etc., and then choose a lender. In auctions, the process is that of the reverse auction, where lenders bid for the customer’s business based on the information that the customer provides. QuickenLoans, OnMoney.com, and GetSmart.com are examples of the banking mall, while LendingTree.com, Priceline.com, and LoanWeb.com are reverse auctions. The hyper-growth in e-lending will tend to force lenders to keep up with lending technology or risk being left behind by the competition. In our information-based society, the question of ownership of key information is an important issue, and one that is to continue causing controversy.

Key Words: E-commerce, e-lending, Information Infrastructure and Internet Services

Introduction To Financial Needs Of A Networked Economy

What is at Stake for the Financial Needs of Consumers?

The reality is finally sinking in that merger deals, however grandiose, do not automatically solve the real problem of banking, which is the continuing loss of business to other types of financial intermediaries. Some CEOs hope to regain lost ground by embracing technology and e-commerce. Others pin their fortunes on improved day-to-day execution, particularly in consultative selling. (Johnson, 2000a, p. 3)
Electronic commerce continues to gain significant increases in consumer usage, confidence and spending, and, although the banking industry has been relatively slow to adapt, its time is fast approaching. A recent Fannie Mae study revealed that, although only 2% of recent homebuyers used the Internet for the entire mortgage process in 2000, half of all Americans anticipate that most home mortgage loans will be handled over the Internet within 5 years. The portion of respondents that would “definitely” or “probably” use the Internet to apply for a mortgage loan was 30%, up from 20% in 1996 (“Online Mortgages May Grow Fast,” 2000). The market for Internet mortgage applications could grow 150% over the next 4 years, to $150 - $200 billion (Bergsman, 2000). However, even with these trends, the state of electronic banking at present is no good. According to Orr (2001c), approximately 10% of all banks offer e-banking in any form, and 90% of banking households are still choosing not to take advantage of handling their financial affairs over the Internet. In 2001, there are about 50 Internet-only e-banks – which most of them are unprofitable, and many are compromising their reason for being by opening physical branches. Orr (2001a, 2001b, and 2001c) suggested that the slow growth of e-banking is mainly due to the fact that banks are slow to offer it, and when they do offer it, they usually do not promote it aggressively. Still, e-banking should be the wave of the future, since demographics are pointing to the next generation that have grown up with the Net. In fact, “All banks, especially large ones, will rapidly shift the bulls eye of their e-banking target to the top 10%-20% of their customers who deliver 70% or so of the banks' profits. The buzzword here is ‘wealth management’” (Orr, 2001c, p.53).

Mortgage lending has so far been the focal point in the e-lending industry, but other areas of consumer credit are emerging. Details from Forrester Research predicts that one of every six credit cards will be issued online by 2003, and that home equity loans, auto loans, and student loans will follow mortgages into hyper growth (Orr, 2000). In fact, online student loans are expected to increase from 12 thousand to 3.3 million, or 25% of all such loans. The graph in Figure 1 shows Forrester Research’s projected market for online credit over the next few years.

Another small, but emerging market for online lending is small business loans. Small businesses are connecting to the Web at an even faster rate than private households (50% are connected, 75% are expected to be by 2002), and about 75% of small businesses need to utilize outside funding to meet working capital and asset acquisition needs (Orr, 2000). Credit scoring models, relying heavily on the owners’ personal financial information, are being used for fast loan approval or rejection. Many small businesses need the convenience of that quick response time. Some lenders approve or reject within minutes for loans of $50,000 or less (Garcia, 2000). Obviously, in order to compete in the Internet market, e-lenders need to consider the benefits to lender and customer, the credit risks, the problems, and the alternatives that are quickly develop in the web-based environment. Some popular e-lenders cope with this environment by being multiple site lenders. “Multi-lender web sites are portals-gateways to affiliated institutions that actually originate loans. Prospective borrowers submit profiles of their intended home purchase and their own financial resources” (Orr, 2000, p. 45). Thus, the
web site serves as a shopping place for borrowers and a source of prospects for lenders, “which seems like a win-win situation” (p. 45). Also, another tactic is to target small business for e-lending. Although until recently, lending to small businesses has not been a high priority for most lending institutions, especially large banks – primarily due to the labor intensiveness of the underwriting process, the high risks, and the relatively small income per loan – this market is especially favorable to e-lending since it minimizes the previously mentioned disadvantages that big banks find in dealing with these relatively small businesses.

**Figure 1: Mortgage lending has so far been the focal point in the e-lending industry, but other areas of consumer credit are emerging** (details from Forrester Research in Orr, 2000)
Reasons Why Lenders Should Consider E-Lending

A primary reason that lenders may consider e-lending is the potential in cost savings. Processing loan applications takes time, personnel, and, therefore, money. E-lending can significantly reduce the amount of time it takes to process loans by allowing the potential borrower to do much of the work, including data entry. The cost savings for thousands of applications per year will be substantial (Warson, 2000). Keep in mind, however, that the start-up costs for e-lending can be significantly cost prohibitive in nature (Britt, 2000). Lenders must be confident of volume projections. E-lending provides another opportunity to gain the much-valued and lucrative “wallet share.” Offering e-lending services to your already savvy Internet customers allows banks to increase the amount of business with that customer. Lenders can use the increased flow of information and real-time interaction to offer a variety of products and services that are relevant to a particular customer (Kassarjian, 2000). E-lending also allows lenders to reach borrowers outside of their traditional market areas.

Finally, the growth in e-lending, as discussed previously, will tend to force lenders to keep up with lending technology or risk being left behind by the competition (Cofran, 2000). Grant Thornton’s annual survey of community bank executives revealed that 28% of respondents were concerned about competition from Internet portals and Internet banks. Only 11% of those surveyed offered online lending services, but 75% said they would establish an Internet lending program within the next three years (Lamb, 2000). In 2001, there are about 50 Internet-only e-banks – which most of them are unprofitable (Orr, 2001c).

Why Consumers Consider E-Borrowing

The major impact of the Internet has been the shift of power from businesses to consumers, who now have unprecedented amounts of information available, and have come to expect unprecedented levels of service. Lending is becoming a self-service industry (Lamb, 2000). Customers are looking to the Internet for many different reasons, and e-commerce companies, including lenders, need to have the capabilities to quickly address all of them. Customers are looking for choice, convenience, security, the ability to quickly compare prices, education about products and services, and speed of service (Waller, 2000). E-borrowers in particular like applying for loans in anonymity. The process frees the borrower from the pressures of dealing with a real person. They do not have to be embarrassed to tell their computer how much debt they have, how much money they make, or how many payments they may have missed. And should the loan be rejected for any reason, customers avoid the shame of being told by a person. This avoidance of embarrassment and shame may mean that riskier customers are using the Internet, so lenders have to be wary (RMA, 2000). There is more discussion of risk later in this paper.
So far, customers’ interests in Internet borrowing have been largely educational in nature (Hewitt, 2000). Hence, as these interested parities gain more confidence in matters of information expertise and security, the acceptance rate of this form of financial transaction could grow exponentially in nature. These interested parties may gather information about loans, rates, repayment options, and competitors, and then go into their bank or credit union fully armed with information. Lenders, therefore, need to make sure that information and education is available and easy to find on Web sites.

**Need for Understanding Internet Customer and Role of Operational Effectiveness**

Banks, and all other e-companies, need to understand the customer. Customer acquisition and retention is the key to e-business, and retention is less costly than acquisition. The groups of customers that use the Internet for banking services has some common characteristics that, if understood, can help banks maximize the appeal of their websites (Rosen, 2000):

1. Internet banking customers tend to be either under 40, or over 55 (retired or semi-retired).

2. Generally, the Internet banking customer want, and even demand, the right to use the Internet, even if it is not their primary delivery channel.

3. Internet banking customers generally want to be left alone to do their business, but, when they need help, they expect it immediately. 24/7 live help has become a right rather than a privilege.

4. Most Internet users are not afraid to use the “chat” mode for help.

5. Internet banking customers are not particularly concerned with the bank’s heritage and reputation, but, rather, about the security, functionality and convenience of the delivery channel.

Typically, one out of two customers abandon Internet banking channels in frustration, citing two basic reasons: It is too complicated, and there is a lack of customer service (Rosen, 2000). According to Rory Rowland, president of Rowland Consulting Services, Internet shoppers tend to move through four basic stages (Waller, 2000):

1. Looking for information

2. Exchanging information about themselves

3. Buying something small

4. Buying something large
A consideration of these stages led to the development of the Continuum Model of Internet Shopping, which is presented in Figure 2. The model shows how consumers move from looking for information to exchanging personal information as they gain confidence in the system, the process, and the provider. Continued confidence and motivation to try a transaction leads to the purchase of something small. Continued confidence, continued motivation, and familiarity lead to the purchase of something larger. The customer then can extend the process into other areas of e-commerce (investing, banking, borrowing, or purchasing elsewhere online.

![Figure 2: The Proposed Continuum Model of Internet Shopping](image)

A key aspect in this continuum model is that once confidence is broken or motivation or familiarity is stifled, the arrows are broken, and the cycle ends. One of the main thrusts of this model is to explain the relative lack of customer service (confidence) or a complex process (motivation) can result in the abandonment of Internet channels. The model builds on the work of Porter (1996, 1999a, 1999b) that states that, although Operational Effectiveness (OE) -- performing similar activities better than rivals perform them -- is necessary for superior performance, there is a difference between operational effectiveness and strategy.
Need for Strategic Foresight and Operational Effectiveness of Porter: Adding Value through Competitive Performance

Strategy should involve performing activities differently than rivals do in order to maintain competitive advantage. As stated by Porter, "a company can outperform rivals only if it can establish a difference that it can preserve, and it must deliver greater value to customers or create comparable value at a lower cost, or do both" (1996, p. 62). Basically, Porter suggested that there is a "productivity frontier", that constitutes the sum of all existing best practices at any given time" (1996, p. 62). This frontier could apply to individual activities, groups of linked activities, and to an entire company's activities, or, in this case, the concept of e-lending. Improving OE moves a company toward the frontier, but this frontier "is constantly shifting outward as new technologies and management approaches are developed and as new inputs become available" (1996, p. 62). In order for e-lending companies to become e-leading companies, there is a need to keep up with this frontier -- managers have been too preoccupied with improving only OE. One tool of OE, benchmarking, ultimately causes companies to begin to look alike -- therefore it is important for e-leaders to think outside the box defined by other financial leaders. Thus, according to Porter, "competitive strategy is about being different" (p. 64) by "deliberately choosing a different set of activities to deliver a unique mix of value" (1996, p. 64). This concept certainly applies to customer acquisition and retention as the key to e-business in general and e-lending in specific, and retention is less costly than acquisition. To support this idea, the classical Southwest Airlines' profitable policy of serving price-sensitive and convenience-sensitive travelers, and also IKEA, which targets young furniture buyers who want style at low cost, are role models that e-leading firms could imitate.

For e-lending institutions to grow in this dynamically changing business and economic environment, a certain degree of strategic foresight is necessary. According to Hamel and Prahalad (1994a, 1994b, 1994c), to develop a prescient and distinctive point of view about the future, senior management must be willing to spend 20 to 50 percent of their time on this subject over a period of months, not days. Senior management "must then be willing to continually revise that point of view, elaborating and adjusting it as the future unfolds" (Hamel and Prahalad, 1994b, p. 65). The first step in this process is the "quest for industry foresight -- a deep understanding of the trends and discontinuities (technological, demographic, regulatory, or lifestyle) -- that can be used to transform "industry boundaries and create new competitive space.” Of course, the trick is to foresee the future before your competition.

From this foresight comes a sustainable vision for the firm. "While understanding the implications of such trends requires creativity and imagination, any "vision" that is not based on a solid factual foundation is likely to be fantastical" (Hamel and Prahalad, 1994b, p. 66). Thus, building industry foresight demands that e-lending management accept the challenges to move beyond the issues on which they claim expert status. The future of e-lending can be found in the intersection of changes in technology, lifestyles, regulation, demographics, and geopolitics. By insight into new product possibilities, and
going beyond traditional modes of marketing research, a firm can develop industry foresight to prosper in the future in a highly competitive environment. Therefore, strategy “is the creation of a unique and valuable position, involving a different set of activities” (Porter, 1996, p. 68). These concepts are partially integrated in the proposed model (Figure 2), so that e-leading “strategy is about combining activities” that “fit and reinforce one another,” and that “fit is a far more central component of competitive advantage than most realize” (1996, p. 70).

**Internet and Its Special Set of Financial Risks**

An audio-conference conducted by RMA, The Risk Management Association (formerly Robert Morris Associates), stressed that while the Internet offers new types of financial rewards for the financial services industry, e-commerce practices also have its own special set of risks (RMA, 2000). Those risks include lower approval rates (every denied application costs money), higher-risk customers, unknown borrowers, and an increased occurrence of fraud. Panelists agreed that, in the “virtual environment,” approval rates fall, because there is greater number of higher-risk applicants. One cause is heavy marketing that leads to heavy volume. Another is anonymity. Higher risk applicants are more likely to apply online since they do not want to be told no face to face (Orr, 2000). The panelists also agreed that fraud on the application is the most common source of risk. Chris Conrad, vice president for fraud management at First USA Bank One (Wilmington, DE), said of fraud that his bank sees little of any other type of risk (RMA, 2000).

The key to combating fraud and higher risk applicants is to remember that banks (and other lenders) determine who will become a customer. Lenders must establish and enforce credit standards with which they feel comfortable (RMA, 2000). Credit bureau information should be used to help identify fraud attempts. Banks need tools that can immediately verify such simple data as name, social security number, address and phone number, and credit bureaus are a good source of such information. Any information that does not match, should raise a red flag. Banks also need to implement training programs in fraud identification.

Banks should use technology to create a database of fraud experience. Many in management are extremely surprised, when they monitored the volume of repeat offenders coming in, how significant a burden it places on the operational effectiveness of the firm. In addition, any detailed discussion of lending risk should be coupled with an equally detailed discussion of interest rates.

In determining interest rates, banks traditionally consider three primary costs: The risk factors inherent in the loan, the administrative costs, and the cost of funds (McDonald and McKinley, 1981). E-commerce companies historically tend to try to compete on the basis of price. In lending, however, price of capital (interest rate) should have a direct relationship with risk. As risk increases, so should the interest rate charged
to compensate the lender for taking that risk. To charge a lower rate of interest on e-
loans, despite a higher level of risk, as discussed above, violates that basic law of lending.

**Special On-Line Lending Problems**

Of course, there are problems other than credit risk. From a customer’s point of
view, security is probably the most important issue. Stoneman (2000) cited a statement
from Richard Biell of TowerGroup: “It’s one thing to submit a credit card number online
to buy a product. It’s quite another thing to put your entire personal dossier online and
hope that no one intercepts it, particularly if you’re not familiar with the lender.” These
confidence and familiarity issues tie into the presented model. A borrower will not
proceed to exchanging personal information without a sufficient level of confidence, and
will not pursue other products and services without being familiar with the vendor and
the process. For lenders, online loan origination volume has so far been underwhelming
(Hewitt, 2000). Volume projections have been under some criticism, largely because
there is not a standard definition of what an Internet origination is. Hewitt (2000) quoted
Fannie Mae’s Michael Williams as saying that if you’re looking for an online origination
volume quote, “you probably can get a quote to match any number you want.”

Another interesting problem that has been making news lately is that of
the ownership of information. For example, in February of 2000, an online lender, e-Loan,
allowed its customers to check their credit scores online. A credit score, a three-digit
number derived by a computer algorithm from a customer’s credit history, can determine
approval or rejection, interest rates, and loan terms. These scores are one of the bases of
fast credit decisions. Fair-Isaac, the credit reporting company, demanded that the scores
are proprietary, and forced e-Loan to stop offering them to customers. E-Loan officials,
the Federal Trade Commission, and consumer advocate groups have been pushing for
legislation to make Fair-Isaac and other credit reporting companies to divulge credit
scores (Bicknell, 2000). Obviously, this paper is not the place for a debate on credit
scores, but the issue clearly demonstrates that, in this information-based society, the
question of ownership of key information is an important issue, and one that is not going
to go away. If customers feel that they have a right to certain information, keeping it
away from them is another way of breaking the arrow in the suggested Model of Internet
Shopping. Customers become frustrated and suspicious. They lose the confidence and,
perhaps more so, the motivation that it takes to pursue Internet transactions.

**E-Lending as Acceptable Alternative in Competitive Environment**

For example, although for most dot.com startups, the last 20 months have been a
nightmare, two Internet-only banks have managed the takeoff phase and climbed to
substantial size and even profitability (Orr 2001a, 2001b). According to Orr (2001a),
NetBank, started in 1996, has more than $1 billion in deposits and its operations have
been profitable for the past thirteen quarters and E*Trade Bank, formed from the
acquisition of TeLeBank by E*Trade, the online brokerage firm, has almost $7 billion in
deposits. However, as suggested by Orr, profitability is rare among the rapidly dwindling
number of Internet-only banks. “Virginia Philipp, an analyst at TowerGroup, identified
40 internet only banks at the beginning of this year. Her ‘hunch’ is that the number is now in the 25-30 range, on its way down to 5-10 within five years” (p. 62). It may be that the best alternative for larger banks is to establish an e-lending presence on their own Web sites -- sites that offer other banking products and services. Many believe that the ultimate winners in the online lending market will be those with both an online and offline presence (Julavits, 2000).

In addition, larger banks tend to instill more confidence in consumers, leading, according to the model displayed in Figure 2, to more online activity by those consumers. Banks should strive to be vertical portals, as described below. If banks plan to survive in the Internet market, they must become more users friendly and provide live customer service. According to the web site at Forbes.com (2000), there are an number of suggestions, including three fairly sensible ways of introducing customers to the convenience, security, and speed of online banking:

1. Place PCs in lobbies so that customers can try the service with real help nearby.

2. Copy the Amazon.com model of using customer information already collected, so that customers do not have to keep entering the same information for credit card or loan applications.

3. Install online help button that immediately connects to a live customer service representative.

Consider the effect that these actions will have on confidence, motivation, and familiarity, the key components for movement through the Continuum Model of Internet Shopping (Figure 2).

Lamb (2000) offered three models for Internet delivery: Aggregators, portals, and specialty providers. Specifically, aggregators are those sites that offer information and products from hundreds of different lenders, some of which may not be depository institutions. These sites can be in the form of malls or auctions. In malls, the customer can do research on products, rates, terms, etc., and then choose a lender. In auctions, the process is that of the reverse auction, where lenders bid for the customer’s business based on the information that the customer provides. QuickenLoans, OnMoney.com, and GetSmart.com are examples of the banking mall, while LendingTree.com, Priceline.com, and LoanWeb.com are reverse auctions (Lamb, 2000).

There is, however, a gap between the promise of aggregators and the reality. Aggregators are not “scouring the planet for great rates”: they are using a finite list of lenders that are paying referral fees (Stoneman, 2000). In addition, lenders using aggregators for loan volume are contributing to the reality that financing is becoming a commodity. Some industry analysts consider aggregators a short-term solution to E-lending, to be used until banks develop sufficient brand recognition to draw customers away (Lamb, 2000). According to Dan Gilbert, CEO of QuickenLoans, who was
recently quoted by Orr (2000), “Multilender sites are not profitable. They don’t work. They never will” (p. 61). QuickenLoans recently purchased Rock Financial Corporation, a leading mortgage originator and abandoned its QuickenMortgage.com aggregator site. Portals are large sites that have a section that offers financial products. AOL and MSN both offer such services. Portals offer access to not only online loans, but also to bill payment services, insurance, and investments. There are some portals that are specifically financial, such as Quicken.com, American Express, and Charles Schwab, along with some strictly Internet banks like CompuBank.com and WingspanBank.com. The range of products available to the consumer is what distinguishes portals from regular banking sites (Lamb, 2000).

Morgan Stanley believes that portals are going to become financial supermarkets. Successful ones will offer Web, telephone, and brick and mortar distribution channels. Charles Schwab is a successful example of this strategy, offering a network of brick and mortar branches and a strong Internet presence (Lamb, 2000; Stoneman, 2001). Specialty providers are those lenders that can distinguish themselves in the Internet market by carving out a certain niche. “The 2000 class of online banks is no longer trying to attract a mass clientele with a universal model. Instead, they are adopting niche-focused models or are teaming up with affinity groups to generate specialized products” (Ptacek, 2000). Specialty providers can market not only through their own sites, but also through aggregators and non-financial sites. PeopleFirst.com has been very successful in the online vehicle financing market. PeopleFirst.com, which can approve an online car loan application in 15 minutes, formed alliances with online auto dealers (like AutoByTel.com and Autoweb.com), information providers (like Kelley Blue Book), and aggregators (like LendingTree.com). In small business lending, Crestmark Bank (Troy, Michigan), a “cashless bank” dealing with commercial transactions, uses a combination of the Internet and personal contact to solicit and sell factoring services and loans (Lamb, 2000).

General Implications, Recommendations and Conclusions Associated with E-Lending

For financial institutions, the Internet redefines the “rules of engagement” for customer interaction, acquisition, and relationship management. The opportunity for forward-looking organizations lies in redefining the role of credit, by exploiting the improved information flow and real-time interaction that the Internet offers. By providing additional services and access to physical-world infrastructure, established players can move competition on the Web away from being merely a pricing issue. (Kassarjian, 2000)

A successful Internet strategy requires both strategic thinking -- strategic foresight -- as well as strategic operational planning – Porter’s operational effectiveness. Despite a slow start compared to other Internet ventures, it is the authors’ opinion that Internet
banking will continue to grow. Those firms that do not address this particular need in the financial area of competition are likely to be left behind in a very short time frame. Hence, there are two primary areas of intensive competitive leverage that lenders need to address in the near future:

1. Integration of Internet, telephone, and branch operations,
2. Security and privacy,
3. Education, and
4. Technology alternatives

By addressing these four areas, lenders can affect the way that consumers are likely to act according to the Continuum Model of Internet Shopping, as displayed in the relationship among company focus and model of Internet shopping component, as graphically represented in Figure 3.

![Figure 3: A relational strategic-fit model between company focus and proposed model of Internet shopping component (Figure 2)](image_url)

Hence, a bank entering the Internet arena needs to understand its needs and expectations, and the delivery costs involved. Most importantly, banks need to integrate Internet operations with all other delivery channels. To the customer, the transition from Internet to call center to branch should appear seamless. Hence, according to Raab (2000),

Despite all the advances in delivering financial services online, there’s one tried-and-true delivery system that customers won’t give up: branches. Banks continue to make investments and upgrades in their brick-and-mortar structures, as customers integrate branch use into a multi-channel approach based on what’s most convenient at any given moment. (p. 12)
Banks must also spend the time and money to invest in security and privacy, primarily because it’s the right thing to do, but also because it is one of the OCC’s top priorities (American Banker, 2000). This means using the latest encryption technologies, tracking technology developments closely, and constantly monitoring and updating processes to ensure compliance with the highest standards. As previously discussed, most Internet borrowers are using currently using the Web for education, to secure information on rates, companies, services, products, and options. Even as more and more originations and closings are done online, education will remain an important part of e-lending. Thus, positive strategies include keeping the customer informed through web presences and shared databases, and making sure that price is a major issue, but not the only issue. Service also comes with a price, and most customers understand that. In mortgage originations, there are four parts to price that customers need to know: The origination fee, the discount fee, the actual rate, and the closing costs.

According to Ernest Knudsen, president of Lowrates USA, a mortgage bank, “Currently, [consumers] think that there’s only one rate, and don’t understand that I can actually make more money on a 7.5% loan than an 8% loan, depending on my fees. The industry needs to explain that” (Quinn, 2000). The overall goal is to provide an Internet portal, but all banks cannot start from there, and in-house technology may not be enough (Habal, 2000). More banks are partnering with new entrants rather trying to develop technology and online capabilities in house, due to the enormous capital outlays and the speed to market as compared to in-house. Habal (2000) basically suggested that people in and out of the banking industry would eventually find core competencies of their organization and try to sell it to others who do not have the same competencies, especially in dealing with IT infrastructures. Hence, IT technologies and its competent management are the keys -- if you do not have it, join with someone who does, or simply outsource. In general, Rosen (2000) suggested some advantages to outsourcing:

1. Staying competitive with bank and non-bank competitors,
2. Avoiding cost and obsolescence,
3. Keeping the cost variable, and
4. Conserving management skill and attention.

Further, Rosen (2000) states that outsourcing is an increasingly viable option for small to mid-sized institutions. This allows banks top talent to focus on core issues of competing in an increasingly crowded and complex brave new world. Of technology, Orr (2000, 2001a, 2001b, and 2000c) reported that the e-lending processes must be designed to eliminate human intervention, or they will not able to handle the problems associated with the transition of hyper growth online. Obviously, e-lenders must start now with strategic foresight, since once hyper growth becomes the norm in the financial world, unprepared bankers will be inundated with applications and fighting for resources to keep pace as a laggard.
References


Customer Loyalty and Privacy on the Web

James P. Lawler, lawlerj@aol.com
Pace University
School of Computer Science and Information Systems
New York, New York 10038-1598

Abstract

This study examines from simulation the effects of the privacy sensitivity of customers, the personalization practices or standards of retailers and the difficulty in locating favorable sites, on the loyalty of consumers to a Web site.

The key finding of the study is that customer privacy sensitivity is a critical success factor that significantly impacts loyalty to a retailer. Customers have higher loyalty to sites that request the least information, while they have lower loyalty to sites that request the most information. Web retailers considering expanded personalization of products or services to customers, through increased personal information, need to rethink their practices. The study also found that difficulty in locating a favorable site is a success factor that impacts retailer loyalty, and that customers have higher loyalty to difficult to locate favorable sites on the Web. These findings are important at a time when consumers are empowered with Web technology to immediately shop competitor sites.

The significance of privacy to loyalty is a factor that needs to be considered seriously by retailers, if they are to compete for loyal customers, and this study furnishes a framework to effectively research loyalty, personalization and privacy on the Web.

Key Words: e-Commerce, Loyalty, Personalization and Privacy

Introduction

The topic of loyalty and privacy on the Web is one that can impact the well being of millions of consumers that shop on the Web. Consumers are empowered with Web technologies, are knowledgeable with numerous options and tools to buy products from retailers, and, with these technologies, tools and options, are the smartest shoppers ever known (Newell, 2000). The loyalty of consumers to a Web site is elusive and is a problem to retailers, because of fiercely innovative competitor sites that sell equivalent products and services.

To comprehend loyalty, Bergeron, who contends that loyalty is the number one problem in retailing on the Web, posits a Loyalty Model, that includes factors of emotional bond, alternative Web sites, product value, frustration, difficulty locating alternate sites, and time investment (Bergeron, 2000). The Bergeron Loyalty Model is an ideal framework to study loyalty.
The framework of the Bergeron model is extended in this study to analyze the following:

Customer Privacy Sensitivity – the sensitivity of the customer to his right to not share information with a Web retailer, that in turn uses the information to increasingly personalize its products and services to the customer, through personalization techniques;

Retailer Personalization Standard – the standard of the Web retailer in respecting the privacy of the customer when requesting information to personalize or tailor products and services to the customer.

Privacy sensitivity of the customer and personalization standard of the retailer are also problems, and considered critical in this study, inasmuch as retailers are responding to the elusiveness of loyalty through one-to-one personalized sales strategies (Peppers and Rogers, 1999). Site personalization necessitates the problem of applying increased demographic, personal and transactional information about the customers, that is perceived potentially intrusive to their privacy. Mismanagement of this information, especially sharing it with other retailers, is a problem that excites customers. Still, the criticality of privacy sensitivity and personalization as factors in Web site loyalty is not proven nor quantified by Bergeron, and this non-quantification is a problem in studying loyalty.

Research into methodologies of leading loyalty theorists (Reichheld, 2001; Seybold, 2001; Windham, 2000), as well as Bergeron, revealed limited quantification of personalization and privacy dynamics as critical success factors in evaluating customer loyalty on the Web. Though surveys show increased sensitivity of customers to retailers who personalize their sites through requested information (Vaas, 2000), only some show sensitivity or non-sensitivity decreasing or increasing loyalty to personalized sites, such as a Price-WaterhouseCoopers survey showing that non-protection of personal information is the most typical event that decreases loyalty (Kapreilian, 2002). The significance of privacy sensitivity to loyalty is not proven in the research.

The focus of this study is to therefore analyze the significance of the effects of privacy sensitivity of the customer and the personalization standard of the Web retailer on loyalty, expanding the Bergeron Loyalty Model. The study additionally initiates analysis of difficulty in locating favorable Web sites from the Bergeron model. This study proves and quantifies the Bergeron Loyalty Model in its initial framework.
Research Methodology

The study introduces the Customer Loyalty and Privacy Synthesis Model (CLPS), that employs simulation in SIGMA and statistical analysis in SPSS as research methodologies, in evaluating the effects of customer privacy sensitivity, retailer personalization standard and difficulty in locating favorable Web sites on loyalty. Simulation as a research methodology is most informative in an analysis of the scope and sensitivity of loyalty, personalization and privacy on the Web. Statistical analysis is helpful in interpreting the simulations in their effect, significance, and predictability.

Experimental Design

The CLPS Model analyzes the effects of customer privacy sensitivity, retailer personalization standard and difficulty in locating a favorable site, on customer loyalty to a Web site, and is conceptually diagrammed in the below Figure 1.

The CLPS Model is a discrete event simulation based on randomness. The model is built, coded and designed to generate output of simulations that test the loyalty hypotheses of the study. The experiment in the model is limited to the privacy sensitivity, personalization standard and difficulty in locating favorable site variables, and hypotheses are formulated to test the significance of these variables in effecting loyalty.

Hypotheses 1a and 1b test how customer privacy sensitivity and Web retailer personalization standard, not cited by Bergeron, predict loyalty to Web retailer sites, and are stated below:

\[ H1a. \text{ Customers with higher privacy sensitivity tend to have decreased loyalty to a Web retailer.} \]

\[ H1b. \text{ Customers tend to have increased loyalty to a Web retailer site that has a high personalization or less requested information standard.} \]

The further hypothesis in H2 tests how one selective factor, cited by Bergeron, effects and predicts loyalty to Web retailers, and is stated below:

\[ H2. \text{ Higher difficulty in locating a favorable Web retailer site, offering similar value in product or service, tends to contribute to increased loyalty effect.} \]
In this experiment, the variables are studied at two levels of loyalty (high and low), stated in the following table:
Table 1: CLPS Loyalty Variables and Levels

<table>
<thead>
<tr>
<th>Loyalty Variables</th>
<th>Loyalty Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>High Loyalty</td>
</tr>
<tr>
<td>Customer Privacy Sensitivity</td>
<td>Low Sensitivity</td>
</tr>
<tr>
<td>Retailer Personalization Standard</td>
<td>High Standard</td>
</tr>
<tr>
<td>Difficulty Locating a Favorable Site</td>
<td>High Difficulty</td>
</tr>
</tbody>
</table>

The three variables, each at two levels, contribute in $2 \times 2 \times 2 = 8$ combinations of variables to be tested in the experiment. The test is defined as a $2 \times 2 \times 2$ factorial design. The experiment with these combinations of variables is stated in the below table:

Table 2: CLPS Loyalty Experiment

<table>
<thead>
<tr>
<th>Independent Variables</th>
<th>Dependent Variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Sensitivity</td>
<td>Loyalty</td>
</tr>
<tr>
<td>High Sensitivity</td>
<td>Low Loyal</td>
</tr>
<tr>
<td>Low Sensitivity</td>
<td>High Loyal</td>
</tr>
<tr>
<td>Personalization Standard</td>
<td></td>
</tr>
<tr>
<td>High Standard</td>
<td>High Loyal</td>
</tr>
<tr>
<td>Low Standard</td>
<td>Low Loyal</td>
</tr>
<tr>
<td>Difficulty</td>
<td></td>
</tr>
<tr>
<td>High Difficulty</td>
<td>High Loyal</td>
</tr>
<tr>
<td>Low Difficulty</td>
<td>Low Loyal</td>
</tr>
</tbody>
</table>

Each of the variables contributes to an equation predicting loyalty, that is explained later in Regression Analysis.

The variables are tested in simulations of customers buying or not buying on a site. That is, customers considering the buying of a consumer durable product or service search the Web for a favorable site, identify the site, and, if satisfied with privacy sensitivity and personalization standard, buy from the site; if a favorable site is not identified, or if privacy or personalization is not satisfied, the customers continue to search for the favorable site from a limitation of sites. The simulations of the customers identifying a favorable site, Web site personalization standard and difficulty identifying a favorable site, or interacting with an identified Web site, are completely random.

Model Implementation

The CLPS Model is built to simulate customers searching and entering retailer Web sites. The criteria for the customer to buy or not buy from a site is based on customer privacy sensitivity (CUSPRIV), retailer personalization standard (WEBPERS) and difficulty in locating a favorable site (DIF), and includes high to low conditions of...
these variables that effect the buying decisions of the customers. The result of the simulations is that if the customers buy high, they are considered high loyal, and if they buy low, they are considered low loyal.

The CLPS Model is programmed in SIGMA.

Customer sensitivity to privacy is defined in the state variable called CUSPRIV. CUSPRIV is also defined by the following sensitivity levels:

CUSPRIV = 3 (High Customer Privacy Sensitivity);
CUSPRIV = 2 (Low Customer Privacy Sensitivity);
CUSPRIV = 1 (No Customer Privacy Sensitivity).

One should note that, without any loss of generality, low and no sensitivity are combined in this simulation into one CUSPRIV = 2 level.

The simulation employs a threshold variable called CUSPRIVTH, the threshold beyond which customer sensitivity to privacy is defined to be high. That is, customers will buy products or services of a Web site if the retailer personalization standard, defined in the state variable called WEBPERS, contains a higher value than the threshold CUSPRIVTH, and they will not buy if WEBPERS contains a lower value than this threshold. The simulation sets arbitrary CUSPRIVTH values for both high and low privacy sensitivity.

For example, in a high privacy sensitivity customer (CUSPRIV = 3), the threshold variable is set high, such as CUSPRIVTH = 0.75, indicating that this customer will only buy the product or service and be loyal if WEBPERS contains a higher value than CUSPRIVTH = 0.75, while in a low sensitivity customer (CUSPRIV = 2), the threshold is set low, such as CUSPRIVTH = 0.25, indicating that this customer will only buy and be loyal if WEBPERS contains a value higher than CUSPRIV = .025.

The conditions of the CUSPRIV / WEBPERS program are summarized in the following table:

<table>
<thead>
<tr>
<th>Privacy Sensitivity</th>
<th>Retailer Personalization Standard</th>
<th>Site Loyalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>CUSPRIV Level</td>
<td>CUSPRIV</td>
<td>CUSPRIVTH</td>
</tr>
<tr>
<td></td>
<td>Condition</td>
<td>Value</td>
</tr>
<tr>
<td>3</td>
<td>High Privacy Sensitivity</td>
<td>.75</td>
</tr>
<tr>
<td>2</td>
<td>Low Privacy Sensitivity</td>
<td>.25</td>
</tr>
</tbody>
</table>
Difficulty in locating a favorable site is defined in the state variable called DIF.

DIF is additionally defined in the following state variables:

DIFTH – threshold beyond which anxious customers having difficulty in locating a favorable site identify an ostensibly favorable site;
NSITE - number of sites searched in locating a favorable site;
FAV - probability customer identifies a favorable Web site.

Loyalty is defined in the DIF simulation by the following values:

LOY = 3 (High Customer Loyalty);
LOY = 2 (Low Customer Loyalty);
LOY = 1 (No Customer Loyalty).

This simulation employs the DIFTH state variable in the search for a favorable site from a limitation of 10 sites. That is, if the number of sites identified prior to a favorable site is high, difficulty to locate the favorable site is considered high, and if the site is found by the customer, and privacy and personalization conditions are satisfied by the site, the customer will buy from that site; if the number of sites prior to the favorable site is low, difficulty is considered low. If the favorable site is not identified in the first nine sites, the simulation sets the tenth to be the favorable site. The simulation sets arbitrary DIFTH values for high and low loyalty and also the arbitrary limitation to 10 sites.

For example, the DIFTH variable is arbitrarily set high to greater than or equal to .66, which corresponds to 7 or greater searches to identify the favorable site, indicating that if this customer identifies the ostensibly favorable site following a search where NSITE is greater than or equal to 7, the customer will buy from the site, and the loyalty effect will be considered high (LOY = 3), while conversely the loyalty effect will be considered low (LOY = 2).

The conditions of the DIF program are summarized in the table below:

<table>
<thead>
<tr>
<th>Number of Sites</th>
<th>Difficulty in Locating Sites</th>
<th>Site Loyalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSITE Search</td>
<td>Search Condition</td>
<td>DIFTH Value</td>
</tr>
<tr>
<td>7 – 10 Sites</td>
<td>High Difficulty</td>
<td>.66</td>
</tr>
<tr>
<td>1 – 6 Sites</td>
<td>Low Difficulty</td>
<td>.66</td>
</tr>
</tbody>
</table>
The CLPS Model generated 544 events in 1,000 minutes (simulation time units), and the output is interpreted next in Regression Analysis.

**Regression Analysis**

From the simulation events, Table 5 notes CUSPRIV generating no LOYALTY cases \((34 + 1 + 103 = 138)\), low LOYALTY cases \((130 + 132 + 33 = 295)\), and high LOYALTY cases \((108 + 3 + 0 = 111)\).

**Table 5: CUSPRIV Simulations**

<table>
<thead>
<tr>
<th>Privacy Sensitivity</th>
<th>Less</th>
<th>Moderate</th>
<th>More</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loyalty Level</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>34</td>
<td>1</td>
<td>103</td>
<td>138</td>
</tr>
<tr>
<td>Low</td>
<td>130</td>
<td>132</td>
<td>33</td>
<td>295</td>
</tr>
<tr>
<td>High</td>
<td>108</td>
<td>3</td>
<td>0</td>
<td>111</td>
</tr>
<tr>
<td>Total</td>
<td>272</td>
<td>136</td>
<td>136</td>
<td>544</td>
</tr>
</tbody>
</table>

Table 6 notes WEBPERS generating no LOYALTY cases \((54 + 32 + 30 + 22 + 0 = 138)\), low LOYALTY cases \((27 + 46 + 65 + 62 + 95 = 295)\), and high LOYALTY cases \((23 + 22 + 25 + 20 + 21 = 111)\).

**Table 6: WEBPERS Simulations**

<table>
<thead>
<tr>
<th>Personalization Standard</th>
<th>.00 – .19</th>
<th>.20 – .39</th>
<th>.40 – .59</th>
<th>.60 – .79</th>
<th>.80 – 1.00</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>54</td>
<td>32</td>
<td>30</td>
<td>22</td>
<td>0</td>
<td>138</td>
</tr>
<tr>
<td>Low</td>
<td>27</td>
<td>46</td>
<td>65</td>
<td>62</td>
<td>95</td>
<td>295</td>
</tr>
<tr>
<td>High</td>
<td>23</td>
<td>22</td>
<td>25</td>
<td>20</td>
<td>21</td>
<td>111</td>
</tr>
<tr>
<td>Total</td>
<td>104</td>
<td>100</td>
<td>120</td>
<td>104</td>
<td>116</td>
<td>544</td>
</tr>
</tbody>
</table>
Table 7 notes DIF generating no LOYALTY cases \((58 + 55 + 14 + 8 + 3 = 138)\), low LOYALTY cases \((175 + 93 + 19 + 8 + 0 = 295)\), and high LOYALTY cases \((39 + 48 + 11 + 8 + 5 = 111)\).

Table 7: DIF Simulations

<table>
<thead>
<tr>
<th>Difficulty</th>
<th>.00 -.50</th>
<th>.67 -.75</th>
<th>.80 -.83</th>
<th>.86 -.88</th>
<th>.89 -.91</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>58</td>
<td>55</td>
<td>14</td>
<td>8</td>
<td>3</td>
<td>138</td>
</tr>
<tr>
<td>Low</td>
<td>175</td>
<td>93</td>
<td>19</td>
<td>8</td>
<td>0</td>
<td>295</td>
</tr>
<tr>
<td>High</td>
<td>39</td>
<td>48</td>
<td>11</td>
<td>8</td>
<td>5</td>
<td>111</td>
</tr>
<tr>
<td>Total</td>
<td>272</td>
<td>196</td>
<td>44</td>
<td>24</td>
<td>8</td>
<td>544</td>
</tr>
</tbody>
</table>

Through interpretation of the simulations in SPSS, the Least Squares Analysis of the data generated by the simulations describing CUSPRIV, WEBPERS and DIF shows strength in the power of the CLPS Model to predict customer loyalty on the Web. In Table 8 below, the R squared value of .436 implies that 43.6% of the variability in LOYALTY is accounted for by the independent variables CUSPRIV, WEBPERS and DIF included in the regression equation, which measures the percentage of variability or performance of the regression. The Adjusted R Squared value of .433, which measures the fit of the model, is close to the .436 R Squared value, reflecting the strong performance of the model and the sufficiency in the number of simulations observed in the model.

Though the .436 R Squared value is low, and 56.4% of the variability in loyalty is not accounted for in the model, an important research direction would be when the other Bergeron loyalty variables of emotional bond, alternate sites, frustration, time investment and value are included in the model, the .436 will get nearer to 1.000.

The Standard Error of Estimate, which measures the accuracy of the predicted values from the regression equation, is a low as .509, which implies that the predicted values will vary slightly around their mean predicted value, improving the accuracy of the CLPS Model with a high level of confidence.
Table 8: Least Squares Analysis

<table>
<thead>
<tr>
<th>R Squared</th>
<th>Adjusted R Squared</th>
<th>Standard Error of Estimate</th>
</tr>
</thead>
<tbody>
<tr>
<td>.436</td>
<td>.433</td>
<td>.509</td>
</tr>
</tbody>
</table>

The R Squared value of .436 supports hypotheses H1a, H1b and H2, in their inclusion of the independent CUSPRIV, WEBPERS and DIF variables that account for the strong dependent LOYALTY variability. CUSPRIV is the variable that tests Hypothesis H1a, that customers with higher privacy sensitivity tend to have decreased loyalty, WEBPERS tests Hypothesis H1b, that customers tend to have increased loyalty to a Web site that has a high personalization standard, and DIF tests Hypothesis H2, that higher difficulty in locating a favorable site tends to contribute to increased loyalty effect. The variables regressed in Least Squares Analysis strengthen the predictability of the loyalty hypotheses.

Table 9 shows Analysis of Variance (ANOVA), which compares averages. The explained Sum of Squares regression value of 108.002 is sufficiently high to study loyalty, though the unexplained residual value of 139.658 indicates the ideal of including the other aforementioned Bergeron loyalty variables not in the CLPS Model, in order to fully study LOYALTY. The positive F ratio of 139.200, measuring overall fit of the model, shows a strong goodness of fit in the data, and the Significance value of .000 shows a 1.000 confidence in the predictor creditability of the model when including CUSPRIV, WEBPERS and DIF.

Table 9: Analysis of Variance (ANOVA)

<table>
<thead>
<tr>
<th></th>
<th>Sum of Squares</th>
<th>df</th>
<th>Mean Square</th>
<th>F</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regression</td>
<td>108.002</td>
<td>3</td>
<td>36.001</td>
<td>139.200</td>
<td>.000</td>
</tr>
<tr>
<td>Residual</td>
<td>139.658</td>
<td>540</td>
<td>.259</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>247.660</td>
<td>543</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*544 – 1 = 543

Of further interest in the study is the interpretation showing that if only one of the CUSPRIV, WEBPERS and DIF variables is included in LOYALTY, and the other two variables are constant, the predictive power of the CLPS Model is shown to be not as strong as when all of these variables are included in LOYALTY.

Table 10 shows a low R value of .096 and a R Squared value of .009 when only DIF is included in the model. A substantial .991 value of other loyalty variables is
excluded from the regression analysis and unexplained when only DIF is included in the model. The Standard Error of Estimate is a higher .673 that limits the predictive strength of the model.

Table 10 also shows the DIF ANOVA regression value to be a low 2.265, and the residual value to be a high and unexplained 245.395. The positive 5.003 in F ratio shows the model is functional, but limited again in its predictive strength. The Coefficient Analysis indicating a .222 value, and a weak positive .099 value, shows a relationship of DIF to LOYALTY, but not sufficient without WEBPERS and CUSPRIV.

The R Squared value of .009 in DIF supports Hypothesis H2, that higher difficulty in locating a favorable site tends to effect increased loyalty, but not the strongest predictability of loyalty without WEBPERS and CUSPRIV.

Table 10: DIF as One Predictor Variable

<table>
<thead>
<tr>
<th>R</th>
<th>R Squared</th>
<th>Adjusted R Squared</th>
<th>Standard Error of Estimate</th>
</tr>
</thead>
<tbody>
<tr>
<td>.096</td>
<td>.009</td>
<td>.007</td>
<td>.673</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sum of Squares</th>
<th>df</th>
<th>Mean Square</th>
<th>F</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regression</td>
<td>2.265</td>
<td>1</td>
<td>2.265</td>
<td>5.003</td>
</tr>
<tr>
<td>Residual</td>
<td>245.395</td>
<td>542</td>
<td>.453</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>247.660</td>
<td>543</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Estimated Coefficients</th>
<th>B</th>
<th>Standard Error</th>
<th>t</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOYALTY</td>
<td>1.836</td>
<td>.059</td>
<td>31.367</td>
<td>.000</td>
</tr>
<tr>
<td>DIF</td>
<td>.222</td>
<td>.099</td>
<td>2.237</td>
<td>.026</td>
</tr>
</tbody>
</table>

Table 11 shows a higher R value of .228 and a R Squared value of .052 when only WEBPERS is included in the model, implying a higher WEBPERS impact than DIF. The Standard Error of Estimate is .658, limiting predictive strength.
Table 11 further shows the WEBPERS ANOVA regression value to be a slightly higher 12.904, and the residual value to be a still high and unexplained 234.756. The positive 29.793 in F ratio shows model functionality, but limited in its predictive strength. The Coefficient Analysis indicating a .525 value, and a weak positive .096, shows the relationship of WEBPERS to LOYALTY, but not sufficient without DIF and CUSPRIV.

The R Squared value of .052 in WEBPERS supports Hypothesis H1b, that customers tend to have increased loyalty to a site that has a high personalization standard, but not the stronger predictability of loyalty without DIF and CUSPRIV.

### Table 11: WEBPERS as One Predictor Variable

<table>
<thead>
<tr>
<th>R</th>
<th>R Squared</th>
<th>Adjusted R Squared</th>
<th>Standard Error of Estimate</th>
</tr>
</thead>
<tbody>
<tr>
<td>.228</td>
<td>.052</td>
<td>.050</td>
<td>.658</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Sum of Squares</th>
<th>df</th>
<th>Mean Square</th>
<th>F</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regression</td>
<td>12.904</td>
<td>1</td>
<td>12.904</td>
<td>29.793</td>
<td>.000</td>
</tr>
<tr>
<td>Residual</td>
<td>234.756</td>
<td>542</td>
<td>.433</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>247.660</td>
<td>543</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Estimated Coefficients**

<table>
<thead>
<tr>
<th></th>
<th>B</th>
<th>Standard Error</th>
<th>t</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOYALTY</td>
<td>1.687</td>
<td>.056</td>
<td>30.149</td>
<td>.000</td>
</tr>
<tr>
<td>WEBPERS</td>
<td>.525</td>
<td>.096</td>
<td>5.458</td>
<td>.000</td>
</tr>
</tbody>
</table>

CUSPRIV, in contrast to DIF and WEBPERS, is shown in Table 12 to be significantly higher in R and R Squared values of .604 and .365 when CUSPRIV is the only variable in LOYALTY, and DIF and WEBPERS are constant. Still, a substantial .635 value of other loyalty variables is excluded and unexplained in the model.

The CUSPRIV ANOVA regression value shows additionally a higher 90.278, and the residual shows a lower and unexplained 157.382, while the positive 310.905 in F ratio, and a negative -.491 in coefficient value, is more functional than DIF and WEBPERS, but limiting again in predictive power.
The R Squared value of .365 in CUSPRIV supports Hypothesis H1a, that customers with higher privacy sensitivity tend to have decreased loyalty to a site, but not the strong predictability of loyalty without DIF and WEBPERS.

### Table 12: CUSPRIV as One Predictor Variable

<table>
<thead>
<tr>
<th>R</th>
<th>R Squared</th>
<th>Adjusted R Squared</th>
<th>Standard Error of Estimate</th>
</tr>
</thead>
<tbody>
<tr>
<td>.604</td>
<td>.365</td>
<td>.363</td>
<td>.539</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sum of Squares</th>
<th>df</th>
<th>Mean Square</th>
<th>F</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regression</td>
<td>90.278</td>
<td>1</td>
<td>90.278</td>
<td>310.905</td>
</tr>
<tr>
<td>Residual</td>
<td>157.382</td>
<td>542</td>
<td>.290</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>247.660</td>
<td>543</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Estimated Coefficients</th>
<th>B</th>
<th>Standard Error</th>
<th>t</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOYALTY</td>
<td>2.810</td>
<td>.054</td>
<td>52.080</td>
<td>.000</td>
</tr>
<tr>
<td>CUSPRIV</td>
<td>-.491</td>
<td>.028</td>
<td>-17.633</td>
<td>.000</td>
</tr>
</tbody>
</table>

CUSPRIV is nevertheless notably higher in regression values than DIF and WEBPERS, implying the higher relationship of CUSPRIV to LOYALTY in the CLPS Model.

Of final interest is the interpretation when all of the predictor variables are included in LOYALTY, the predictive power of the CLPS Model is shown to be the strongest.

Table 13 shows the coefficients of strong negative CUSPRIV and strong positive WEBPERS and DIF variable values.
Table 13: Coefficient Analysis – All Predictor Variables

<table>
<thead>
<tr>
<th>Estimated Coefficients</th>
<th>B</th>
<th>Standard Errors</th>
<th>t</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOYALTY</td>
<td>2.348</td>
<td>.078</td>
<td>30.037</td>
<td>.000</td>
</tr>
<tr>
<td>CUSPRIV</td>
<td>-.491</td>
<td>.026</td>
<td>-18.683</td>
<td>.000</td>
</tr>
<tr>
<td>WEBPERS</td>
<td>.585</td>
<td>.076</td>
<td>7.731</td>
<td>.000</td>
</tr>
<tr>
<td>DIF</td>
<td>.330</td>
<td>.076</td>
<td>4.317</td>
<td>.000</td>
</tr>
</tbody>
</table>

The coefficients in Table 13 contribute to the following LOYALTY regression equation:

\[
LOYALTY = 2.348 \text{ (average of LOYALTY with CUSPRIV, WEBPERS and DIF constant at zero)} - .491 \text{ CUSPRIV (lower LOYALTY with more customer privacy sensitivity)} + .585 \text{ WEBPERS (higher LOYALTY with high retailer personalization standard [less requested information])} + .330 \text{ DIF (higher LOYALTY effect with more difficult to locate favorable sites.)}
\]

The negative -.491 coefficient in CUSPRIV in the equation supports the negative relationship to loyalty stated in Hypothesis H1a, that customers with higher privacy sensitivity tend to have decreased loyalty to a Web retailer. The positive .585 coefficient in WEBPERS supports the positive relationship to loyalty stated in Hypothesis H1b, that customers tend to have increased loyalty to a site that has a high personalization standard.

The positive .330 coefficient in DIF supports the positive relationship to loyalty stated in Hypothesis H2, that higher difficulty in locating a favorable Web retailer tends to contribute to increased loyalty effect.

The strong CUSPRIV, WEBPERS and DIF coefficients in the regression equation show the strength in the relationship of these independent predictor variables to the dependent LOYALTY variable and support the hypotheses of the study.

Managerial Interpretation

The CLPS Model confirmed that privacy sensitivity and retailer personalization standard are significant factors in loyalty on the Web. The regression analysis indicated that customers fundamentally sensitive to their right to not share information with a retailer have lower loyalty to the retailer, while those not sensitive to their right have higher loyalty. Loyalty was further impacted in the analysis that indicated customers have lower loyalty to a retailer that requests the most information, while having higher loyalty to a retailer requesting the least information. The joint impact of the analysis confirmed customer privacy sensitivity and retailer personalization standard as significant factors effecting loyalty to a Web site, supporting Hypotheses H1a and H1b of the study.
The implication is that consumers are not trusting of the privacy standards of Web retailers.

This analysis is important to Web retail management in its implementation of personalization practices. If customers are sensitive and not initially trusting of the practices and privacy standards of the retailers, they will not be loyal to the site. Though the retailer practices may be only annoying and not always intrusive, the threat will be high, due to the simple Web empowered option to surf to other Web sites perceived to be trusting.

At the same time, the CLPS Model confirmed that the Bergeron factor of difficulty in locating a favorable site selling equivalent products and services is a significant factor in loyalty. The regression analysis indicated that customers have lower loyalty to less difficult to locate favorable sites, and higher loyalty to more difficult to locate favorable sites. The impact of the analysis confirmed difficulty in locating sites as a significant loyalty factor, supporting Hypothesis H2.

This analysis is also important to Web retail management, but limited in benefit in a study of loyalty. If customers are highly sensitive to the privacy standards of a retailer, and there are competitive retailers, the customers will surf to these sites if they are not difficult to locate on the Web. If these sites have privacy standards not intrusive to the customers, these customers may be loyal to the sites, excluding other loyalty factors.

However, what if these sites subsequently alter their privacy standards to be competitive in personalization techniques, but insensitive to highly sensitive customers, will these customers surf to other sites, reconcile themselves to their newly found insensitive privacy sites or return to the initial insensitive site? Such customers will be elusive in their loyalty, irrespective of their selected sites, and the retailers would be misled if they thought these customers to be truly loyal to them.

Retailers need to consider that customers will not be loyal to their sites only because competitor sites were difficult to locate on the Web. Once the competitor sites effect ease of location, the consumers will surf to them, supporting the theme of the study that loyalty is elusive on the Web.

**Conclusion**

The key finding of the study is that the privacy sensitivity of the customer is a critical success factor that significantly impacts loyalty to a retailer. Customers have higher loyalty to sites that request the least information, while they have lower loyalty to sites that request the most information. Web retailers considering expanded personalization of products or services to customers, through increased personal information from their customers, need to re-think their strategy. The CLPS Model confirms studies in non-academic sources (Pew, 2000) that show customers increasingly sensitive to personalization techniques that intrude upon their privacy. Inasmuch as most retailers personalize their sites, but only half of them rate their personalization practices
poor to fair in satisfying their customers (Pfenning, 2001), insensitivity to this issue will erode the loyalty of the customer to the Web site.

At the same time, the study shows the finding that the Bergeron Loyalty Model factor of the difficulty in locating a favorable Web site is a critical success factor that impacts retailer loyalty. Customers have higher loyalty to difficult to locate favorable sites. This finding is important, in that the Bergeron model in this initial factor is shown to be a quantitatively supportive tool for researchers and retailers to study loyalty.

A further overall finding is that although customer privacy sensitivity, retailer personalization standard and difficulty locating favorable sites contribute individually to loyalty, none contribute solely to loyalty. Only when these factors are included collectively is the CLPS Model initially creditable in explaining loyalty on the Web. Feasibility is high that when the other Bergeron factors of emotional bond, number of alternative sites, value, frustration and time investment are included in the CLPS Model, the Bergeron Loyalty Model will be a substantially creditable framework to study loyalty on the Web.

Though it is not clear if these subsequent Bergeron factors will be higher in criticality than privacy sensitivity, the CLPS Model shows in the least that privacy sensitivity is not a negligible factor in loyalty. Inclusion of privacy sensitivity of the customer and related personalization standard of the retailer as critical success factors in loyalty strengthens the Bergeron model.

In short, the Customer Loyalty and Privacy Synthesis Model (CLPS) is meaningful to researchers and retailers who will study loyalty and privacy in the framework of the Bergeron Loyalty Model.

References


Applications and Process Strategies of Bar Coding Technologies in the Health Care Industry

Alan D. Smith, smitha@robert-morris.edu
Robert Morris College
Department of Management and Marketing
Moon Township, PA 15001

Abstract

Information technology and automated inventory control have changed payables, receivables, and the asset side of inventory. Although more layers of security measures, such as tougher access control and new encryption schemes, may be needed to guard against computer criminals than ever before, automatic data collection techniques, such as biometrics and bar coding schema have distinctive advantages in the applied health and health-related services sectors. Reduced Space Symbologies (RSS) and Composite Symbologies are relatively new technologies, that should produce higher accuracy levels, better information gathering and reduced exposure to costly litigation. Efficient Healthcare Consumer Response, for example, found that $23 billion of the $83 billion-a-year health care purchasing market was spent on moving products from factory to hospital bedside, and $11 billion could be reduced immediately by adopting new technologies and standards, such as UPNs. Future trends are discussed and the suggestions for further research in health care and bar coding are given.

Key Words: Automatic Data Collection, Health Care and Bar Coding Techniques and Information Technologies

Introduction

Information Technology and Automated Inventory Control: Historical Context

A growing number of firms that manufacture and/or sell consumer products are testing technologies that could transform the way industries use the Internet to track goods in their supply chains -- in specific, automatic identification. For example, a MIT Auto-ID project is spearheaded by some of the world's largest consumer packaged goods, retail and computer companies -- International Paper, Procter & Gamble, Sun Microsystems, Unilever and Wal-Mart -- and is supported by the Uniform Code Council, a standards body that represents companies in 23 industries (Semilor, 2001). The management of information technology as well as business is all about promoting linking and connectivity in organizational structures. In its simplest form, management must link products to orders and orders to shipments and shipments to payments. The use of the Internet and automatic identification and data capture systems serves as a foundation for management of data flows for strategic purposes, such as using bar codes in distribution warehouses as well as other basic transactions that both cause and result from this informational and resulting material flows. For example, bar codes, a form of automatic identification and data capture system, can be linked via the Internet in combination to
identify each different product, and, through the extensive use of bar codes, can be used to link a container moving throughout a supply chain to the database controlling it. Since “bar codes are demanded in industries, such as manufacturing, healthcare and pharmaceuticals, distributors hesitant to risk getting involved in the bar code market should reconsider” (Kemler, 2001, p. 69) their position. Through the process of replacing vast amounts of information normally processed by human workers that are prone for errors with scannable bar code symbologies, end users are able to significantly reduce handling time and transposition errors. In addition, since the information is recorded and stored in a real-time fashion, end users will acquire a greatly enhanced and accurate tracking in the supply chain, as compared with traditional manual methods.

An inspection of technological changes, in term of supply chain management over the last 20 years, has illustrated that there have been tremendous changes in the area of physical distribution or supply chain management systems through global businesses. Information technology and automated inventory control systems have changed payables, receivables, and the asset side of inventory. Typically, at the highest level, an enterprise resource planning (ERP) system manages the data, while bar code scanners collect the needed information and pass it on up to the ERP system. Unfortunately, the new data capture system proved to be as much an obstacle to entering data as the old manual methods, since the scanners read the bar codes but did not complete the connection to the ERP system. The solution that Kohler Company (1 million square foot distribution center in Sheboygan, Wisconsin) found was to move to cordless scanners and decoding wedges that had a track record with Kohler's specific ERP system – currently, the database reflects inventory levels in real time (“Kohler cuts data capture time 80%,” 2001). This setup gave workers equipped with cordless scanners move to the inventory, rather than the other way around. ERP screens are installed at the workers’ user interface, assisting workers by allowing them to visually follow the data capture process, with audio effects to alert workers the condition of data entry.

On the consumer side, changes in information technology allow firms to collect data on who buys what and for what price and to find out what consumers want to buy (Benfield, 2001). In addition in a classical work by Swanson (1994), there are at least three major ways these IS innovations can occur: Process innovations occur which are confined to the IS core; Products and services are added to support the administrative core of the business; and Products and services are integrated with core business technology.

Recently, logistics has created significant scale opportunities. In attempts to do more with less more accurately, firms have developed warehouse automation, RF communication systems, and new bar-coding mechanisms. For example, Wal-Mart is a famous example of a company taking advantages of scale to offer lower prices than the competition. Developing its own satellite system, Wal-Mart uses extensively a bar coding system to take advantage of scale. Products are moved directly from warehouses to stores without a middleman. A middleman would diminish the scale of distribution for
Wal-Mart and reduce profits – which allows for sustainable competitive advantage, through continuous e-commerce and IT infrastructure improvement, via automatic identification and data capture technologies.

**Major Advantages of Using Automatic Data Identification and Data Capture Technologies: Bar Coding**

Also recently, new developments are being implemented to improve customer responsiveness and increase efficiency. Synapz, for example, has recently launched Eclipz version 1.3 (“Synapz enhances Web-based Eclipz product for automotive supplies,” 2001). This system enables automotive suppliers to manage the flow of data between thousands of supplier companies. Allowing them to receive orders, confirm shipments, and send orders via the Internet does this. Suppliers have the option of receiving e-mails when a customer firm sends e-mail for new orders. This means suppliers do not need to sign on to the Internet several times a day. Finally, companies now have the ability to print container bar-code labels for shipments. The label can include shipping notice information. This allows customer firms to simply scan the contents for the containers without opening them or opening up shipping forms.

Bristol Myers Squibb has adopted a machine-readable code called “Snowflake”, which consists of a pattern of dots that can be read using a machine vision system. Snowflake codes are reproduced using printed labels, laser etching, indenting, and hole punching (Woods, 1997).

Bar coding technologies also allow companies to standardize much of the traditional supply chain activities. This, as mentioned above, allows companies to increase economies of scale and standardize global operations. For example, in early January, 2001, Zebra Technologies (Hills, 2001), the worldwide leader in bar code printing solutions, offered to assist GM to develop label templates that can be used globally for routing all parts to and within GM plants. These labels are designed, using Zebra’s expertise, to assure compliance with GM’s shipping label standards. This new automatic identification system maximizes the use of bar coding to streamline operations. This in turn allows these companies to improve productivity, reduce costs, and therefore increase profits.

In addition to other tangible benefits of automatic identification and data capture technologies, bar coding allows companies to be more efficient in operations. It allows companies to update inventories in real time. For example, Toyota replaced a manual data entry tracking system with a system using portable bar printers and handheld wireless terminals. Before the system was implemented, it could take two weeks to enter data into a computer manually, and during that time, cars could not be moved. Now information can be immediately updated in real time, and cars can be immediately moved. Also the manual system was prone to error. If the vehicle identification number (VIN) was 14 characters long and typically Toyota processed 26,000 cars a year, missing one number on the VIN could possibly mean searching for that car for days. Bar code labels can include the time, date, and location of the scan, a 5- digit tracking number, and
information about the model, color, and options. This information is automatically updated as the product is tracked. This information can be used for such functions as invoicing, loan information, and inventory control. It also allows the company to keep track of when any damage occurs to the product. Yao and Carlson summarize nine areas where bar coding helps companies:

1. Communication systems can provide very detailed and accurate up-to-the-minute logistical information.

2. Up-to-date screen reporting replaces batch printout reporting.

3. RFDC terminals can be mounted on equipment and are highly portable.

4. Information can be integrated for quality information service leading to increased profits.

5. Standardized procedures make inventory operations easier to be managed, adjusted, and upgraded.

6. Inspection data and quality control data can be added to the bar code labels for processing, analyzing, and distributing in a matter of seconds.

7. Management can partner with both suppliers and customers to make processes more efficient.

8. Systems engineers and designers can assign grades to all tasks that involve people to make better relationships between management and labor.

9. The pipeline of information can be continuously studied, evaluated, and improved to effect continuous improvement in operations management (Yao and Carlson, 1999).

Applications to Health Care

Personal Digital Assistants (PDSs) and other computers that can be held in the hand, provide a way to send information to caregivers in a very timely manner. Bar coding is developing at a rapid pace (Noble, May, 2000). Medical diagnostic products of blood analysis, for example, can provide critical diagnostic information to healthcare professionals accurately and immediately. This can occur at the point of patient care, not three weeks later. Also, prescription writing and medication management programs can help to decrease errors in prescription transcription, especially when there can be adverse effects due to errors. This also helps to control costs due to more accuracy of information (Paul, 2001).

Bar coding can be used, furthermore, in all segments of the health care system, not just for patient care. All segments of the health care system are under pressure to conform to the widespread use of UPN within their industry, in terms of patient/supply...
chain applications. Manufacturers of medical/surgical and pharmaceutical products are also receiving an increased pressure to apply UPN-compliant bar codes to their product. The application of bar codes can then be used throughout the supply chain, right to the patient. There must be a sustained and systematic approach for developing and implementing a UPN bar code labeling-program within the health care industry. Strategies for increasing process efficiencies, improving quality, international labeling, and gaining label control are just a few of the many ramifications of automatic identification and data capture technologies. Applications are in the market that address coding and billing issues, and this helps to alleviate the administrative load during the medical treatment process. Also, applications that were once only available on the mainframe are now as portable and as accessible as a cell phone (Noble, 2000). This should improve revenues, reduce costs, and increase the likelihood of regulatory compliance -- at the regulatory side of health care is going to get more complex in the future. This is important, since it appears the bar codes are an essential component in the product identification and flow of goods and information in electronic commerce, as illustrated in Figures 1 through 3. The Uniform Code Council (UCC), in conjunction with its European counterpart (EAN), provides standardization and issues guidelines and company identification numbers.

The UCC issues are based on the binary system. Bar code symbology is based on character set, type, element widths, length or density, with self-checking techniques. Although there are many symbologies available, only a few are in common use, and regulated by industrial specific organizations (see Table 1 for common symbologies used in traditional bar-coding applications).

### Table 1: Common Symbologies for Bar-Coding Applications

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPC</td>
<td>Commercial, retailing</td>
</tr>
<tr>
<td>Code 39</td>
<td>Industrial, military, health</td>
</tr>
<tr>
<td>Interleaved 2 of 5</td>
<td>(ILF) shipping, distribution</td>
</tr>
<tr>
<td>Code 128</td>
<td>Distribution, health care</td>
</tr>
<tr>
<td>PDF 417</td>
<td>Portable data file was in medical records, product documentation</td>
</tr>
<tr>
<td>Data Matrix</td>
<td>Component marking, hazardous materials</td>
</tr>
<tr>
<td>Maxicode</td>
<td>Shipping and distribution, high speed sorting</td>
</tr>
</tbody>
</table>
Figure 1: UPC (Universal Product Code) and EAN (European Standards) Bar Codes

Figure 2: UCC (Uniform Code Council) / EAN - 14 in Interleaved 2 of 5 (ITE) Bar Code
In addition, space limitations on small healthcare items made it very difficult to bar code complete item information. As demonstrated in Figure 4, the Uniform Code Council and EAN International have been working with the leaders of the global healthcare industry to utilize Reduced Space Symbology (RSS) and Composite Symbology, as the solution for space-constrained identification in healthcare. This relatively new RSS symbology should produce higher accuracy levels, better information gathering and reduced exposure to costly litigation. The quality of patient care will be tremendously enhanced (Roberts, 2001). Hence, collecting data at the bedside and sharing it in real time can also avert all kinds of disasters. This increases both efficiency in operations and improved patient care. A hand-held automated blood analyzer, for example, combines established principles of electrochemistry with micro-fabrication process technology -- from the semiconductor industry). This allows professionals to draw a few drops of blood to perform the full panel of standard blood tests at the patient’s bedside. The professional can also scan the patient’s id bracelet and access information or enter new information. This information includes such data as vital statistics and medication administration events. Caregivers can also view electronic medication administration records entered on other dates.

Companies like NextRx System are developing new systems that unify automation, bar coding, and wireless to reduce medication errors and save money. NextRx’s new system provides health care institutions an automated approach to reducing medication errors and increasing efficiency. NextRx System’s bar coding system innovations uses multiple quality checks to assure accuracy when bar coding is used to receive, inventory, and pick and safely administer medications (“NextRx announces launch of nation’s most comprehensive . . .” 2000).
The key to management of these new systems is combining bar coding with wireless technology, which the author will refer to as “wireless coding.” Howcroft and Mitev (2000), for example, summarized the nature and use of electronic connections used by physicians as the following: Electronic link to reporting authorities, Connection to pathology results, Internet links, Electronic services, General administrative tasks, Repeat prescriptions, Computerized patient records, Clinical coding, Storage of pathology laboratory results, and Consultation with patients. Automatic identification and data capture technologies, coupled with wireless coding connections and schemas, should result in supply chain benefits found in the manufacturing environment apparent in health care institutions.

**Case Study: Bar Coding System to Reduce Medication Error**

For illustrative purposes, the Veterans Affairs Medical Center in Washington, D.C. has recently deployed a new system to reduce medication errors through bar coding. This system needs to be used with wireless local area networks (WLANS). Unfortunately, many wireless application technologies, such as cellular phone operations are banned in most hospitals due to the potential interference with medical devices.
Pager networks offer bandwidth suitable only for a limited amount of alphanumeric data. Therefore WLANs offer substantial benefits by transmitting data between devices (like a PDA and a nearby desktop computer). The costs of the WLAN are primarily a function of square footage to be covered and the potential wave interference of walls and materials, but other factors affect transmission as well. These factors typically include the following: The physical characteristics of the building involved; Competing technologies and their technical configurations; The kinds of devices employed; The number of devices employed; and how the work is to be organized (Yacoe, 2000). Hence, many hospitals are currently engaged on a campaign to “unplug doctors and nurses.” Wireless systems extend services from the nurse’s station to at least 25 feet.

The application of this technology allows staff to offer more timely care, so that patients want to come to the hospital, doctors and nurses are happier, and hospitals are being sued less – an effective use of human capital. For example, the Veterans Affairs Medical Center is concerned with the problems commonly associated with inventory management and patient registration. This system tracks the administration of bar-coded medications within 172 VHA hospitals in the United States. The costs have been around $18,000 to $25,000 for a 20-bed ward. The total cost for the system was $360,000. This covered the antennae for the network, purchase of scanning devices, adding wireless cards to laptops, and equipment changes in the pharmacy (Yacoe, 2000). Bar coding, along with WLANs used in combination with the wireless network, reduced medication errors at Washington Veteran Affairs Medical Center over 23 percent – a very significant improvement, considering the moral and legal ramification of error in this already well-monitored environment.

Although allied health officials inspected the prospects of primitive bar-coding medications in the early 1990s, recent applications have evolved to the point where a physician can enter a medication order into a computer, send that simultaneously to the pharmacy, and also send it to a nurse’s medication cart. The laptop on the cart shows which medications are ordered for each patient. It also shows what time the medication should be administered. A scanner on the cart checks the bar code on the medicine right before giving it to the patient, to make sure there are no mistakes in switching bottles by mistake, and that there are no mistakes in administering the medication at the wrong time or the wrong number of times.

**Industrial Analysis: Need for Error Reduction**

Some current statistics estimated that between 44,000 and 98,000 deaths may be attributed to medicine error in U.S. hospitals on an annually basis (“ADC—it could be a matter of life and death,” 2000). More than 7,000 are from medication errors – which includes prescribing, dispensing, and administering the wrong drug or dosage and administering a drug at the wrong time. Interestingly and not surprising, the Institute of Medicine identifies the utilization of bar coding as an effective remedy to these types of errors. Bar coding ensures the identity and dose of the drug are as prescribed by the attending physician, given to the right patient, and that all the steps of dispensing and administering the drug are checked for timeliness and accuracy (“ADC—it could be a
matter of life and death,” 2000; Beaker, 2001a, 2001b). Bar coding succeeds by replacing handwriting, manual data input, and human interpretation. Bar coding provides a means to record medications immediately and to increase tractability. Hence, according to Howcroft and Mitev (2000, p.179), application of this technology can be completed without affecting the relationship with patients and the ways in which physicians perform their duties

**Future Trends in Bar Coding Schemas in Health Industry**

The Health Industry Business Communications Council (HIBCC) is promoting bar code provider application and supplier labeling standards for the health industry. Standards produced by this organization allow providers to employ bar code technology to create a hospital-wide system that connects numerous departments and functions relating to patient care. This obviously reduces the likelihood of error. Hence, pen-based computers could disappear, leaving smaller and more powerful devices to take the place on clumpy and bulky machines, such as hand-helds and portable machines. When third-generation wireless services are pervasive, it may be possible to have a big-screen tablet with a low-power processor. This may be possible in the near future, perhaps in three to five years. Thus, IT departments will need to take competitive advantage of the new 3-G technology to support portable thin-client computing. For example, Microsoft is currently supporting a pen tablet as the platform of choice (Turek, 2001). Costs on uniquely designed bar code systems are constantly falling (Becker, 2001a). Efficient Healthcare Consumer Response, for example, found that $23 billion of the $83 billion-a-year health care purchasing market was spent on moving products from factory to hospital bedside, and $11 billion could be reduced immediately by adopting new technologies and standards such as UPNs. In fact, more than 93 percent of medical supplies on hospital shelves appear to have universal product numbers on them -- at least while still in their boxes and there a great potential for huge savings in supply-chain in this sector (Becker, 2001a). In addition to costs savings, computer security issues in health care institutions are especially sensitive to management of such IT applications.

In general, security is a concern in information systems, especially in legacy systems that may be more vulnerable to various computer crimes. This has become a vital issue since the September 11, 2001 tragedy. The leap in computing power may create a big gap between businesses equipped with the latest technologies and those who are not so equipped in executing automatic data collection and data capture technologies. Those businesses that lag behind will be extremely vulnerable to attacks, such as data tempering and viruses – which in the health care industry would be crippling. Since modern computers and their associated ERP systems -- enterprise resource planning, such as Oracle -- are especially sensitive to changes in the environment, it is entirely possible for hackers to disable or damage systems, not just through software, but also through magnetic disturbances and heating of the environment. Prevention will be ever more counted upon as a major role of any IT department, especially the applied health fields and any industry that utilizes sensitive and personal databases. In addition, prevention against inadvertent damage to systems might be also required. Hence, multiple layers of security measures, such as tougher access control and new encryption schemes, may be
needed to guard against computer criminals than ever before. In addition to criminal tampering, non-criminal damages in the automatic data identification and data capture loop may result in tremendous obstacles as well.

Spectra Science Corporation is developing new bar coding labels designed to withstand challenging environments and to continue to provide accurate identification of a product throughout its life cycle (“Spectra Science and Kleen-Tec Industries establish agreement...” 2001). The end result of this innovation is that hospitals’ labels may withstand repeated washings when equipment and bedding are cleaned. LaserCode labels basically use a hybrid technology that leverages signal-to-noise advantages of light emission with the high code densities of the bar coding process. Each label contains a series of lines that emit one of several wavelengths to represent a unique number. This allows for a high level of tolerance of soil and wash fading, due to that fact that the label emits wavelengths of light rather than reflecting light. In addition, in an unique application of biochemical bar-coding by Freemantle (2001), bar-coded microrods are prepared by sequential electrochemical reduction of metal ions into the pores of an alumina membrane template with a silver film at its base.

At an even more sophisticated systems-level application, exciting future trends are occurring at McKesson HBOC. McKesson HBOC is expanding its Internet offerings with a new service called Supply Management Online. McKesson pioneered the use of information technologies in healthcare supply management and distribution with customer order management, bar coding, and hand-held device solutions. Now, with its Supply Management Online, PDA devices can be used to order, receive, and make available both pharmaceutical and medical-surgical products and information to online services health care customers. Graham King explains, “Today’s procurement systems offer a fragmented view of purchasing activities across the enterprise. Supply Management Online helps fill the gaps by integrating information services, [and by] providing seamless, end-to-end fulfillment” (“McKesson HBOC launches initial phase of virtual marketplace...” 2001, p. 1).

Implications and Suggestions for Future Research

Unfortunately, as suggested by Becker (2001 b), while UPNs, whose electronic conversions into bar codes are widely recognized by consumers, are greatly credited for keeping inventory and warehouse shelves under supply-chain management requirements in the retail industry, the health care industry is far behind their retail counterparts. “But the hospital industry has struggled to standardize, blaming the failure at least in part on suppliers that cloak their products in a jumble of coding that ostensibly protects proprietary information such as pricing” (p. 16). The application of basic wired and wireless bar coding applications for health care institutions, especially in the potentially booming segment for nursing homes, appears to be essentially limitless. A more extensive review needs to be conducted to audit current IT applications and the extent to which bar coding applications are being used in nursing homes, across international as well as domestic borders, especially in the area of the daily administering of medications via a med cart/lap top and the efficient control of inventories -- including such varied
items as medicines, laundry supplies, and kitchen food. In addition, since nursing homes have many patients who require the same dosage of medication over and over, automated systems can certainly cut down on errors and help nursing homes become more efficient. They can also help patient services as well, since family members can be more relaxed about their loved ones not receiving the wrong medicine, when a caring family member is not there to ensure confidence on the patient’s care.

Certainly in the review of the literature in automatic data identification and data capture technologies, the use of bar coding can be categorized according to the type of system involved. This may be completed according to the typology developed by Swanson (1994). How many products and services are integrated with core business technology? How many hospitals even rely on IT beyond the billing department? What are some of the new developments in this area?

Finally, what have been the advantages for nursing home profits and patient services for those nursing homes that take advantage of wireless coding? What is the best way to measure the success of a wireless coding system? How can nursing homes monitor how well their system is performing? The answers to these questions may be grounded in the need to gaining insights into the application of bar coding techniques in the health sector, especially in the area if medication administration in nursing homes – sometimes a much neglected application of IT that could represent numerous improvements in overall nursing home operations. More importantly, this type of research will also allow nursing homes to make higher profits and provide better patient services, in a time when the demographics in the United States points to a large increase in the elderly population. The obvious aging of the affluent baby boomer population should equate into an increased demand for efficient and latest technology, based on automatic data identification and data capture technologies in nursing homes. This trend should prove a great advantage in nursing home administration, as well as in the entire health sector, in order to provide competitive advantage in a modern and frequently chaotic and innovative world.

References

“ACCPAC introduces integrated wireless warehouse management for the mid-markets” (2001) Canada Newswire Ltd., May 7,


“NextRx announces launch of nation’s most comprehensive automated medication distribution system for hospitals” (2000) Healthwire, December 5.


“Toyota keeps its costs down boy bar coding arriving cars and ensuring they don’t stay long on the port’s lot” (2001) *Modern Materials Handling*, April 1.


Right of Privacy and Advertising: U.S. and E.U. Conflicts

Roy J. Girasa rgirasa@pace.edu
Pace University
White Plains, New York

Abstract

The article compares the increasing divergent views of the legal and ethical parameters between the European Union (“EU”) and the United States concerning advertising over the Internet. Continental Europe has always been far more restrictive than the U.S. concerning a number of areas of advertising, particularly, comparative advertising and advertising to children. The Internet has created a Pandora’s box of privacy issues that has been addressed by governments. The recent comparative developments in this area will be reviewed.

Introduction

The U.S. and countries comprising the EU have been on a collision course concerning the right and scope of advertising to consumers within their respective domains. The basic reason for the conflict is the different philosophical and legal traditions underlying the laws and regulations. U.S. advertising law has as its basis the rights guaranteed by the First Amendment of the U.S. Constitution, namely, “Congress shall make no law…abridging the freedom of speech, or of the press…. The Fifth Amendment provides in part: “No person shall…be deprived of life, liberty, or property, without due process of law….” The due process right was extended to the states comprising the United States by virtue of the Fourteenth Amendment which provides: “[N]or shall any State deprive any person of life, liberty, or property, without due process of law….” The result of the Amendments and their interpretation by the courts has been to permit a very broad spectrum of freedom to advertisers. European countries, though respecting individual rights, do not have the tradition of an expansive, if not exaggerated, freedom of speech. For example, it is far more difficult to establish a case arising out of libel or slander in the U.S., especially from a criminal law perspective, than it is in Great Britain, from which U.S. law initially emanated, or from other countries in Europe.

The Internet has created legal problems of extensive magnitude. In past decades, there were many ways to ascertain and file personal characteristics of individuals in various data banks, such as credit agencies. Nevertheless, laws and regulations limited their scope and usage. Until the late 1960s, abuses of privacy were not very widespread owing to the difficulty of accumulating and disseminating data beyond localized areas. Gradually, a number of statutes were passed that modified the then prevailing view of caveat emptor (“let the buyer beware”) legal principle to one of caveat vendor (“let the seller beware”). Congress and state legislatures enacted protective measures that gave consumers some legal protections against abusive companies. Examples of such
legislation are the Truth-in-Lending Act of 1969 that compelled lenders to disclose the annual percentage rate charged for loans; the Fair Credit Billing Act that required creditors to advise debtors of their rights concerning bills rendered to consumers especially arising from credit cards; the Equal Credit Opportunity Act that prohibited discrimination in lending practices; the Fair Credit Reporting Act that gave consumers the right to question unfavorable data in credit reporting agency files and related rights; and statutes prohibiting abusive collection practices. Although these laws were greatly beneficial to consumers, the Internet opened the gate to panoply of other, more difficult to regulate, abuses.

The Right of Privacy

Although implied in certain sections of the U.S. Constitution, there is no right of privacy explicitly guaranteed therein. The first known scholarly review of the subject was written by Samuel D. Warren for the Harvard Law Review in 1890 in an article entitled “The Right to Privacy.” His concern arose from the yellow journalistic accounts about members of his family. In the article, Warren espoused his belief that an individual had the right not to have one’s thoughts, statements, or emotions be made public with consent from the affected persons. The present climate of a century later was pronounced in a most quoted statement of Scott McNealy, CEO of Sun Microsystems, who stated: “You have zero privacy anyway. Get over it.” Is the statement true? Do domestic and foreign laws offer some modicum of protection?

The Meaning of Privacy

There are many definitions of privacy discussed by authors. Two authors, David Banisar and Simon Davies, suggested that there are at least four categories of privacy, namely: (1) information privacy - privacy concerning personal data such as medical and credit reports; (2) bodily privacy - privacy concerning drug testing and the lie; (3) communications privacy - privacy with respect to e-mails, telephone conversations, and other communications methodologies; and (4) territorial privacy - privacy of one’s workplace or other public space. A discussion of privacy must also take into account whether the invasion is by private persons or by governmental authorities. There are stricter protections concerning governmental invasions than by private persons—government intrusions face a number of constitutional safeguards respecting the affected individuals. Individuals have the right to be free from such intrusions by government surveillance, as well as the right to privacy as to public disclosure by government of private information (e.g., one’s tax returns) and freedom concerning one’s thoughts and beliefs (Whalen v. Roe, 429 U.S. 589 (1977)).

U.S. Federal and State Judicial and Legislative Privacy Protections

As stated hereinafore, the U.S. Constitution does not grant explicit privacy rights. Nevertheless, there have been significant developments emanating from judicial decisions that have given a loose framework of constitutional safeguards. For example, in the case of Griswold v. Connecticut, 381 U.S. 479 (1965), the Supreme Court nullified a
state statute that forbade the use of contraceptive devices. In the well-known case of *Roe v. Wade*, 410 U.S. 113 (1973), the court overturned a state law prohibiting abortions. In doing so, the court discussed the constitutional status of the right of privacy. It stated:

> The Constitution does not explicitly mention any right of privacy. In a line of decisions, however, going back perhaps as far as…(1981), the Court has recognized that a right of personal privacy, or a guarantee of certain area or zones of privacy, does exist under the Constitution. In varying contexts, the Court or individual Justices have, indeed, found at least roots of the right in the First Amendment…in the Fourth and Fifth Amendments…or in the concept of liberty guaranteed by the first section of the Fourteenth Amendment…. These decisions make it clear that only personal rights that can be deemed “fundamental;”…are included in this guarantee of personal privacy.

Privacy rights are not exempt, however, from government intrusion, although courts will exercise what is known as a “strict scrutiny” standard that provides that the government must show a clear need for the legislation or action that clearly outweighs that of the individual. Thus, in *Whalen*, the Supreme Court upheld a New York law that classified potentially harmful drugs in five schedules: from the first category, as exemplified by heroin that has no known beneficial use and thus is banned, to lower categories with increasing permissible usages. All prescriptions for the listed drugs had to be registered so as to prevent a person from going to several physicians to wrongfully acquire numerous prescriptions. The court said that although the legislation had some effect upon the individual’s right of privacy, nevertheless, the exhibited need for regulation outweighed the individual’s right to the dissemination of such information. Other examples of privacy wherein a court determines that the government did not act impermissibly were decisions upholding the right of a state to require persons convicted as sex offenders to register and update changes concerning their home address (*Akella v. Michigan Dept. of State Police*, 67 F. Supp. 2d 716 (E.D. Mich. 1999)) and the conduct of a warrantless search of office computers wherein employees were previously informed that electronic audits of computers would be taken periodically (*United States v. Simons*, 206 F.3d 392 (4th Cir. 2000)).

**Federal Statutory Provisions.** There is no right of privacy in U.S. legislation that covers the broad spectrum of privacy rights. Protection is scattered among a number of legislative enactments that cover a variety of abusive conduct that the Congress wanted to curb. Among the laws passed that are specifically directed to the protection of privacy rights are:

*The Privacy Act of 1974* - The Act gave individuals the right to ascertain what records concerning them were collected, maintained, used, or distributed by federal agencies. Individuals were given the right to commence litigation where there was
intentional or wrongful misuse of the said records. The Act was undermined by the numerous exceptions contained in the statute that, in essence, protected police authorities under the guise of security and other related excuses.

The Children’s Online Privacy Protection Act of 1998 - The purpose of the Act was to enhance parental role in protecting the privacy of their children. Among the abuses that caused the Congress to address were the unscrupulous methods advertisers used to gather information concerning the children’s household. Children were often asked by advertisers in cyberspace chat rooms, home pages, and the like, identifying information concerning the size of the household, its likes and preferences, and other personal data all of which was collected without parental consent. A “child” under the Act is an individual under the age of thirteen years. Identifying information includes the first and last name, home and e-mail addresses, telephone number, social security number, a “persistent identifier” such as an identification number, a cookie, a screen name, or other identifying information that allows possible physical or online contact with the child.

The Act makes it unlawful for an operator of a website or online service directed to children to knowingly collect personal information from a child unless: (1) it provides notice on the website of the nature of the information collected; (2) how such information is to be used; and (3) the operator’s disclosure practices for the information. In addition, the operator must obtain verifiable parental consent for such collection, use, or disclosure. Upon request and verification of the identity of the parent whose child has given personal information, the operator must provide a description of the information given by the child, an opportunity to refuse further use or collection or maintenance in retrieval form, and a reasonable means for a parent to obtain such information.

It is also forbidden for such website or online service to condition a child’s participation in a game, the offering of a prize, or other activity on the child giving more information than necessary for participation. The operator must establish and maintain reasonable procedures for compliance with the said restrictions.

There are a number of exceptions for compliance with the statute:

(1) Information received to a specific request from a child on a one-time basis and the information is not maintained in retrievable form and not used anew to re-contact the child;

(2) Requesting information for sole purpose of using it to obtain parental consent or for providing notice and is not maintained in retrievable form;

(3) Responding to a child’s contact beyond one occasion, provided reasonable efforts are made to provide the parent with notice and giving the parent a reasonable opportunity to request no further use be made of the information; or, in the absence of notice to the parent, where the benefits to the child of access of information and services outweigh the risks to security and safety to
the child’s privacy [for example, information regarding abortion services, preventive sexually transmitted disease data];

(4) The name of the child and online contact information to protect the safety of a child and such information is not used to recontact the child and is not disclosed on the site; and

(5) The collection, use, or dissemination of the information is necessary for the security or integrity of the website, is taken as precaution against liability; is used to respond to judicial process, or otherwise allowed by law.

There is a safe harbor provision for the website or service provider that exempts it from liability if it complies with a set of self-regulatory guidelines issued by representatives of the marketing or online industries. The said guidelines must include “an effective mechanism for the independent assessment of subject operators’ compliance with the guidelines” and “effective incentives” for compliance, such as disciplinary action, consumer redress, voluntary payments to the U.S. Treasury for violations, and referral to the Federal Trade Commission of operators violating the guidelines. The voluntary guidelines require approval of the FTC. Industry groups must maintain records that are to be available to the FTC containing customer complaints, records of disciplinary actions, the results of independent assessments of members’ compliance.

*The Gramm-Leach-Biley Act* of 1999, Title V, restricts banks and other financial institutions from disclosing personal information received from their customers to third parties without their consent. Each bank is required to have a privacy policy whether or not it is engaged in the transfer of such information to third parties. Banks are specifically forbidden from disclosing account numbers or access codes to third parties for purposes of telemarketing, direct mail marketing, or e-mail marketing programs.

*The Electronic Communications Privacy Act* of 1986 makes it unlawful for any person to intentionally intercept, attempt or hire another person to intercept any wire, oral, or electronic communication. Thus, tapping phones wherein the interceptor is not a party is unlawful. It is also illegal to disclose information received as a result of the intercepted information if one knows that the information was unlawfully obtained.

*The Right to Financial Privacy Act* of 1999 prohibits governments from obtaining financial records from a financial institution unless they have been lawfully subpoenaed or received pursuant to a search warrant. Financial institutions may not voluntarily surrender or disclose such records to governmental authorities unless they have received written assurance that the governmental authorities have complied with the statute. As in other enactments there are a number of exceptions concerning release for reasons of unlawful activities, proving a debt, and other related exceptions.
The Video Privacy Protection Act of 1999 makes it unlawful for videotape service providers (e.g., Blockbuster) from disclosing information concerning the rentals or purchases of consumers of videotapes without their consent.

The Driver’s Privacy Protection Act makes it unlawful for a state department of motor vehicles to disclose personal information concerning a registrant without a justifiable purpose (presumably to an attorney investigating or gathering evidence concerning an accident).

State Regulation. Individuals are protected concerning their right of privacy in a number of contexts. Most states have enacted uniform laws that incorporate prohibitions found in the Restatement, Torts (Second), Sections 652A-E. They provide as follows:

(1) Section 652B. Intrusion upon Seclusion defined as: “One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person;”

(2) Section 652C. Appropriation of Name or Likeness. “One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy;”

(3) Section 652D. Publicity Given to Private Life. One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public; and

(4) Section 652E. Publicity Placing Person in False Light. One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if (a) the false light in which the other was placed would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false conditions of the matter.

The “intrusion upon seclusion” is exemplified by persons committing, without proper authorization, the act of tapping another person’s telephone, being a “peeping Tom,” reading another person’s mail, and so on. The “appropriation of name or likeness” is illustrated by a case previously litigated by this author. The client, a model who had a photo portfolio made for use in applying for related jobs, found one of her photos placed without authorization in an advertisement in an unsavory man’s magazine. The photo was in an ad soliciting the purchase of a book discussing ways to engage female companionship. Such usage not only was made without consent or monetary reimbursement but also was a source of significant embarrassment to the model.
“Publicity given to private life” refers to the act of publicizing non-public information about a person such as alleged indebtedness owed by such person, or that such a person has AIDS, or other private data. The fourth tort, “publicity placing person in false light” is similar to the tort of defamation and requires that wrongful information be publicized about another that is untrue.

**Federal Trade Commission Initiatives.** The Federal Trade Commission Act of 1914 created the Federal Trade Commission (FTC). Its mandate initially was to prevent unfair methods of competition in interstate of foreign commerce. Later its jurisdiction was expanded to investigate and prosecute unfair or deceptive acts affecting such commerce. In the past five years, the Commission has been concerned with problems associated with online privacy and the attempts by industry to self-regulate. The May 2000 Report to Congress entitled *Privacy Online: Fair Information Practices in the Electronic Marketplace* sets forth the current state of privacy rights in online commercial activity.

In its 1998 Report to Congress, the FTC summarized and identified core principles with respect to privacy protection that are generally agreed to in model codes, guidelines, and government reports. There are four such principles identified therein. They are:

1. **NOTICE** - data collectors must disclose their information practices before collecting personal information from consumers;
2. **CHOICE** - consumers must be given options with respect to whether and how personal information collected from them may be used for purposes beyond those for which the information was provided;
3. **ACCESS** - consumers should be able to view and contest the accuracy and completeness of data collected from them;
4. **SECURITY** - data collectors must take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use; and
5. **ENFORCEMENT** - the use of a reliable mechanism to impose sanctions for noncompliance with these fair information practices.

“Notice” is the most basic principle and underlies the remaining three principles.

**Web Sites Privacy Disclosures.** In early 2000, the FTC conducted a survey of the major industry sites (sites with 39,000 or more different visitors) on the Internet to ascertain the consumer protection privacy policies. Using a random sampling of all sites and an examination of the 100 busiest sites, it found that nearly all sites collected personal identifying information from consumers (97% of random sample and 99% of the 100 most popular sites). 68% of the sites of the random sample and 77% of the most popular sites collected non-identifying information. From the data, detailed information concerning buying behavior and other data were collected. The Commission noted that there was a significant increase (from 14% to 66%) of at least one privacy disclosure in
1999 in the random sample from the prior year. The percentage is expected to rise to 88% in the year 2000. Approximately, 97% of the most popular sites posted a policy in 1999.

The difficulty perceived by the FTC is that less than half of the most popular sites implemented the four core principles of notice, choice, access, and security. Also, many sites posting a privacy policy contained poorly drafted disclosures. Often, language was contradictory or ambiguous or was confusing to consumers. Sites typically reserved the right to change their policies thereby undermining consumer confidence in their privacy policy. The FTC recommended to Congress that these principles be incorporated in legislation to ensure adequate protection of consumer privacy online. With respect to Notice, it recommended that web sites be required to give consumers notice of the information practices in a clear and conspicuous manner. Such information should include what information is being collected; how it is to be collected; how the above principles of Choice, Access, and Security are to be provided; whether the information collected will be disclosed to other entities; and whether other entities are using the web site to collect information.

As to Choice, the web sites would be required to offer consumer choices as to how the information is to be used beyond the stated use, including internal secondary uses such as marketing back to consumers, and external secondary uses, such as giving the data disclosed to other entities. The Access given to consumers is to include a reasonable opportunity review the information and to correct inaccuracies or delete information contained therein. Reasonable steps are to be taken to ensure the Security of all data collected. The FTC is wary of detailed, specific legislation and desires instead that any legislation be made in general terms and be technologically neutral. It wants flexibility in promulgating rules and regulations in keeping with developments as they may take place.

The Law of Advertising and the First Amendment

Prior to the 1970s, commercial advertising had virtually no protection under the Constitution. The first significant indications that the Supreme Court was ready to extend First Amendment protections to certain commercial activity took place in a series of cases beginning in 1973 wherein the Supreme Court overturned the conviction of a newspaper publisher who, before the Roe v. Wade abortion decision, permitted the advertisement of New York abortion services in his Virginia newspaper. The Supreme Court said in Bigelow v. Virginia, 421 U.S. 809 (1975), that although couched in commercial advertisement, the subject matter was one that the public had a right to know. The application of First Amendment freedom of speech and press to advertisements was expanded to include the right to advertise drug prices by a pharmacy (Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, 425 U.S. 748 (1976)), the right to advertise legal services by attorneys (Bates v. State Bar of Arizona, 433 U.S. 350 (1977)), and the advertisement of contraceptives.
European Union Initiatives

European Union Directive 95/46/EC.

The European Union has the strictest privacy protection restrictions in the world. Its Directive, 95/46/EC, sets forth a mandatory minimum of protection to be given by Member States to their inhabitants. Underlying the Directive was its predecessor document known as the Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data that had been adopted by the Organization for Economic Cooperation and Development (“OECD”), as early as 1980. The Recommendation became the basis for such protection in a number of Member States, the Council of Europe, and the United Nations. Part Two of the Recommendation established limits with respect to the collection of personal data, requiring it be done lawfully and with knowledge and consent of the data subject where appropriate. The personal data had to be relevant for the purpose for which it is gathered and is accurate, complete and up-to-date. The data should not be disclosed other than for the essential purpose underlying its collection. The data should be protected by the use of reasonable security safeguards against unauthorized access or use. The individual, about whom the data is collected, should have the right to ascertain whether data has been collected about him/her; have the data communicated to the individual at a reasonable charge in a form that can be understood; be given reasons for denial of such information; and have the right to challenge inaccurate data and have it rectified. Part Three of the Recommendation requires Member States to consider the implications of domestic processing and re-export of personal data for other Member States. Transborder flows of such data should be uninterrupted and secure. With certain exceptions, a Member State should permit unrestricted transborder flows of personal data between it and another Member State and avoid passing laws creating obstacles to such transmission. The OECD Principles concerning collection of data, data quality, use, openness, and safeguards became the basis for international goals, codes and statutes.

The E.C. Directive sets basic requirements for data protection, allowing Member States to enact stricter standards. The effective date for implementation is October 25, 1998. A number of Member States had not yet enacted data protective laws when the Directive was issued. Moreover, the laws of Member States that did enact such measures differed substantially, thereby causing potential obstacles to the free flow of data and difficulties for the inhabitants therein. The Directive was enacted to remove such obstacles, harmonize the national provisions, and guarantee the right of privacy.

Part of the basis for the Directive are the provisions of the Treaty on the European Union that provides in Title I, Article F, that the E.U. “shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on November 4, 1950.” Article 8 of the Convention provides:

(1) Everyone has the right to respect for his private and family life, his home and his correspondence; and
(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

_Scope (Article 3)._ The Directive concerns “any operation or set of operations which is performed upon personal data.” Exceptions include data flowing outside of the European Union and data involving state and public security. “Personal data” is defined as “any information relating to an identified or identifiable natural person (‘data subject’).” The obligations are imposed upon the “controller” who is any person determining the purposes and means of processing data.

_Data Quality Principles (Article 6)._ The Directive provides that Member States are to ensure that the personal data is: (1) processed fairly and lawfully; (2) that it is collected for specific and legitimate purposes; (3) relevant and not excessive for the intended purposes; (4) accurate and kept up to date when relevant; and (5) kept for no longer than necessary except when kept for historical, statistical or scientific use in which case appropriate safeguards are to be enacted.

_Criteria for Legitimacy (Article 7)._ Personal data may be collected only if:

(1) The data subject has consented unambiguously (agreed freely after being adequately informed);

(2) It is necessary for contract performance involving the data subject (for example, data for job applicants or for billing purposes);

(3) It is necessary for compliance with a legal obligation of the controller;

(4) It is necessary to protect the vital interests of the data subject;

(5) It is necessary to carry out a task in the public interest or for exercise of official authority involving the parties (for example, by police or tax authorities); or

(6) For legitimate interests of the controller or third party receiving the disclosure that outweigh the protection of the legitimate interests of the data subject.

_Prohibited Data (Article 8)._ Member States may not collect personal data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life. There are exceptions to such prohibitions including consent from the data subject and legitimate and lawful
objectives and persons. For example, health professionals need health data for proper diagnosis, police authorities need data concerning prior convictions, and journalists may require background data.

**Information to be Given to Data Subject (Articles 10 and 11).** The Directive provides different criteria of information to be given to the data subject depending on whether the data was obtained from the data subject or from some other source. If the data is derived from a third party, the data subject is entitled to know the identity of the controller and his/her representative; the purposes, thereof; and additional information such as categories of the data concerned, the recipients or groups of recipients of the data, and the right of access. If the data is from the data subject, s/he is entitled to the same type of information plus information as to corrections of errors. Exceptions are made for collection of data for historical or scientific research purposes.

**Right of Access to Data and Exemptions (Articles 12 and 13).** The data subject is entitled to know whether or not data about him or her is being collected, the purposes thereof, the categories of the data, and the recipients, as well as how to rectify, erase or block data. There are exemptions for national and public security, defense, prevention, detection, and prosecution of criminal offenses, and for economic or financial interest of a Member State.

**Miscellaneous Provisions: Right to Object (Article 16).** The data subject has the right to object on compelling legitimate grounds to processing of data about him or her. S/he also has a right to object on request and free of charge any data to be given to direct marketers.

**Confidentiality and Security (Article 17).** Member States are to ensure that agents of controllers not process data except on instructions from the controller. Measures are to be taken to protect the security of the data from accidental or unlawful destruction, alteration, unauthorized disclosure or access and all other unlawful uses.

**Remedies (Articles 22-24).** There are broad remedies available to the data subject for violation of his/her rights under the Directive, including judicial access and claim for damages.

**Notification and Exemptions (Article 18).** Controllers or representatives thereof are to notify Member States of automatic processing operations of their names, addresses, the purposes of data collection, and other such information. Exemptions are permitted where the data are unlikely to adversely affect the data subject. Among the exemptions are Article 3(2) that states the Directive does not apply to data falling outside the scope of E.U. law, to wit, in matters of public security, defense, state security, and matters pertaining to criminal activities. Article 13(2) also exempts member states from permitting access to data by the data subjects with respect to scientific research and for the collection of statistics. The third exemption provision is that of data transfer to non-member states.
Data Transfer to Non Member States (Articles 25-26). Data is not to be transferred to countries outside of the European Union, unless those countries ensure “an adequate level of protection.” What is “adequate” depends on all of the attending circumstances of the transfer, including the proposed processing operations, the level of security, its professional rules, and other such qualifications. Nevertheless data can be sent irrespective of such safeguards if the data subject consents; the transfer is necessary in connection with contract performance between parties of the respective countries; on public interest grounds; is necessary to protect the vital interests of the data subject; and where the controller assures protection of privacy concerning the data being sent abroad.

Safe Harbor Provision. The promulgation of the Directive created a great deal of concern in the international community whose laws and regulations are not as restrictive as those found in the Articles of the Directive. The fear was that Member States of the E.U. would enjoy unlimited access to data arising with the E.U. but countries outside of the region would be deprived of the data. The basis for the fear was Article 25 that concerns the transfer of data to outside the E.U. It provides in part that “Where the Commission finds…that a third country does not ensure an adequate level of protection…Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question” [Art. 25(5)]. There were a number of exceptions to the restrictions including consent of the data subject, the data is pursuant to a contract, and other such exceptions. Negotiations took place between the E.U. and U.S. Government representatives that culminated in an agreement on March 15, 2000 that provided for a seven-year window wherein data may be exchanged between E.U. and U.S. companies unless such data is misappropriated or misused by the latter.

In order to qualify for the safe harbor provisions, U.S. organizations that receive personal data from the E.U. have a number of ways in which they may avoid violations of the Directive. They may join a self regulatory privacy program that adheres to the E.U. principles; they have their own self imposed regulatory privacy policies that comply with the Directive; if the latter, a failure to comply with such privacy may run afoul of the Section 5 “unfair and deceptive” practices of the Federal Trade Commission Act; they may be obligated by statutory, regulatory, or other regulatory U.S. body provisions, such as registered securities associations; or they may include the E.U. principles in written agreements with other parties that transfer data from the E.U.

The United Nations previously adopted Guidelines Concerning Computerized Personal Data Files on December 14, 1990. While leaving to individual countries to issue and implement regulations concerning computerized personal data, it issued a series of principles that should guide each State’s initiative. Included among the principles were those of: lawfulness and fairness, accuracy, legitimate purpose, access, and non-discrimination. The Council of Europe adopted the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data on October 1, 1985. It also sets forth a series of principles very similar to those later outlined in the Privacy Directive of the European Union. In addition thereto, Article 14 of the Convention provides for assistance to data subjects residing abroad. It states that each party to the Convention shall give to such persons aiding in exercising the right to ascertain the
existence of a personal file on him/her, its content, and to make corrections or erasures of
data violating his or her privacy rights. Argentina enacted a statute in December 1996
giving data protection (“full protection of personal information”) in conformance with
another law giving its inhabitants the right to obtaining formation about data collected on
them. In addition, a Bicameral Commission on Monitoring of Data Protection was
established to enforce the statute. Australia and Belgium, as members of the OECD,
enacted a statute in conformity with its principles. Hong Kong, prior to its takeover by
the People’s Republic of China, enacted a Personal Data (Privacy) Ordinance that is still
in effect and is reflective of the E.U Directive. The same types of protection may be
found in the statutes and ordinances of many other countries. Japan, Taiwan, and Hong
Kong have enacted measures to insure the some degree of protection concerning the
accumulation and processing of personal data. Among the measures that have been
enacted are: (1) In Japan: *The Act for Protection of Computer Processed Personal Data*
*held by Administrative Organs* (December 1988); (2) In Taiwan: *Law Governing*
*Protection of Personal Data Processed by Computers* (July 1995); and (3) Hong Kong:
*The Personal Data (Privacy) Ordinance* (September 1995).

**E.U. Advertising Directives**

The E.U., in determining that advertising goes beyond the member states’
borders, issued directives concerning misleading and deceptive advertising as well as
comparative advertising Council Directive 84/450/EEC (September 10, 1984). It was also
concerned that the need to complete the internal market required that there be uniformity
concerning the regulations governing the said forms of advertising. Misleading
advertising by reason of the diverse media is prohibited under the Directives.
“Misleading advertising” is defined in Article 2(2) of the 1984 Directive as “any
advertising which in any way, including its presentation, deceives or is likely to deceive
the persons to whom it is addressed or whom it reaches and which, by reason of its
deceptive nature, is likely to affect their economic behavior or which, for those reasons,
injures or is likely to injure a competitor.” Article 3 states that the determination of
whether advertising is misleading shall be based on a number of factors, such as
information concerning the characteristics of the goods or services, their availability,
composition, fitness for the purpose intended, material features, price, and the nature and
rights of the advertiser.

Misleading advertising is not subject to the First Amendment stringencies of the
U.S., although member states have somewhat broad authority to regulate within their
borders. The E.U. had to balance the former prohibitive measures of certain member
states that had banned comparative and/or advertising directive to children with the
demands of industry and member states that permitted such advertising. The need to
conform to international conventions concerning the protection of copyrights also had to
be redressed. Accordingly, comparative advertising, defined under the 1997 Directive,
Article 1(3) as “any advertising which explicitly or by implication identifies a competitor
or goods or services by a competitor” is allowed provided that the advertising is not
misleading, is objective, compares relevant features of the products, does not discredit or
denigrate the competitors’ marks or products, and/or does not take unfair advantage over them.

Member states are required that “adequate and effective means” be taken to combat offenses as proscribed by the Directives. Included among the remedies is legal action against the advertisers to include injunctive relief of cessation of the advertising if already accomplished or prohibition from publication if the advertising has not taken place. In addition, member states are to provide administrative review of complaints by consumers with appropriate relief when mandated. The television directive (Council Directive 89/552/EEC, while permitting advertising to children, makes such advertising subject to certain prohibitions including prohibitions of urging children to purchase or persuade their parent to purchase the advertised products or be exploitative or dangerous to them.

Consumers in the U.S. often possess no reasonable remedy for redress. Purchases made over the Internet rarely allow for satisfactory remedies in the event of fraud or dissatisfaction. Use of Small Claims Court proceedings is limited to jurisdictional authority within the locale of the vendor. Thus, an aggrieved party would have to go to the hometown of the defendant party in order to seek relief. The E.U. has attempted to resolve the difficulty of redress by providing for a “European Consumer Complaint Form” that guides consumers in formulating their claims for resolution by judicial and non-judicial bodies. The U.S. has no such remedial provisions. Individual states through their Attorneys General do provide some relief, albeit scant and only when numerous complaints have been made concerning specific vendors.

Conclusion

Combining the twin concerns of the protection of consumer privacy and protection against false and misleading advertising, including that of comparative advertising, it is apparent that the E.U. has taken the lead in affording relief. The U.S. appears to be more reluctant in providing consumer protection with respect to remedies for privacy violations and restrictions concerning advertising, especially to children. Courts in the U.S. have enforced apparent unconscionable clauses in clickwrap and shrinkwrap contracts. Shrinkwrap agreements are agreements whereby a purchaser of goods becomes subject to the restrictive licensing terms that state the purchaser must agree to or else return the purchased product within a short designated time period. They are most often found in the purchase of computer wherein consumers open the box; find a plastic wrapped package of booklets including the restrictive licensing terms that may, among other terms, provide that any disputes are to be resolved by an arbitration association found often in a distant state. A clickwrap agreement is the same type of agreement whereby the consumer, when opening a new program on a computer, is required to agree to license restrictions before the consumer is able to download the program. Courts have generally found such agreements that consumers nearly always ignore and rarely understand. See, e.g., ProCD v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996) and Crispi v. The Microsoft Network, L.L.C., 323 N.J.Super, 118 (N.J. App. Div. 1999).
The E.U. appears to be more consumer friendly in refusing to have consumers bound by agreements that they either do not understand or where contractual clauses unfairly weigh heavily against them. The U.S. may claim that it is a more open society that necessarily includes access to data that would be deemed private in nature in the E.U. Whether the surrender of privacy concerns in favor of openness is an issue that needs to be addressed in the future.

References


Restatement, Torts (Second), Sections 652A-E.


Aims and Scope of the Journal

The Journal of e-Business and Information Technology is a semiannual international journal which aims to publish articles of high quality dealing with how online business technologies relate to the information technology, addressing various e-business forms and their evolution, and covering all aspects of IT, particularly those touching the Internet.

The intention of the Journal of e-Business and Information Technology is to help the local and global business communities to efficiently exploit IT towards the creation of business value in e-business. The journal welcomes all types of applied research studies in global computing that add value to e-business owners, customers, developers, and evaluators. That is, applied studies in IT, online business technologies (all e-business forms, e-commerce, etc.), and Internet security are particularly sought.

Areas of interest for the Journal include:

-all forms of e-business
-EDI
-e-commerce
-Decision Support
-Data Warehousing
-Data Mining
-Biometrics
-Internet Security
-Cyber Law
-Knowledge Management
-Information Security Auditing

Relevant manuscripts from the field of IT, not in the areas of the Internet or online business technologies, are also considered if they bear implications for the creation of business value in e-business.
The audience of the Journal are members of the local and global business communities, researchers, students, and industrial practitioners doing global computing.

**Preparation of a manuscript submission**

Five copies of the manuscript should be sent to the Editor-in-Chief or one of the Associate Editors of the Journal.

Manuscripts should be printed on 81/2x11” paper, one side only, leaving 1” margins on all sides. Please single space all materials, including footnotes and references. Number pages consecutively with first page containing the title, the authors, the affiliations, a short abstract (between 150 and 300 words), and five to 10 key words.

It is important that your abstract and key words are as most informative as possible since they are used in identifying appropriate reviewers for your manuscript.

**Exclusivity of submission**

The first page of the manuscript should include the statement “This manuscript has not been submitted elsewhere in identical or similar form, nor will it be during the first 6 months after its submission to the Journal of e-Business and Information Technology.”

**Illustrations**

Only clear reproductions of artwork should be submitted. Authors should keep original artwork until the manuscript is accepted. All figures should be in a form suitable for reproduction.

Each figure and table must be mentioned in the text and numbered consecutively using Arabic numbers in the order of appearance in the text. For the initial submission of the manuscript, the figures and tables should be integrated into the text as much as possible, rather than being inserted at the end of the manuscript.
References

References should be inserted, for books, journals, and articles in proceedings, and technical reports, as follows


Permissions

Authors are responsible for obtaining permission from copyright owners if they use an illustration, table, or lengthy quotes from material published elsewhere. The authors should write to both the publisher and the author of material they are seeking to reproduce.

Copyright

The copyright will be established in the name of Pace University.

Offprints

Each author will receive a free copy of the Journal issue containing the published article.

Further information

Further information may be obtained by writing (see address below) or emailing to the Editor-in-Chief at braggad@pace.edu or by accessing http://www.aimit.org.

Bel G. Raggad, Editor-in-Chief
861 Bedford Road
School of Comp. Sc. and IS
Pace University
Pleasantville, NY 10570
Phone#: (914) 773-3448
Please note that starting Jan 2003, the Journal of eBusiness and IT will be published online.

BelRaggad
In this issue:

E-Lending: Foundations of Financial and Consumer Marketing in an Information Intensive Society

Alan D. Smith and William T. Rupp, Robert Morris University

…..Customer Loyalty and Privacy on the Web

James P. Lawler, Pace University

Applications and Process Strategies of Bar Coding Technologies in the Health Care Industry

Alan D. Smith, Robert Morris University

Right of Privacy and Advertising:
United States and European Union Conflicts

Roy J. Girasa, Pace University