EConsumer

Bipin C. Desai

Abstract— **The genuine benefit of the Internet is its ability to make vast amounts of information readily available and thence easy to manipulate, sort, and compile. This ability has been channeled over the last few years to develop Internet based commerce, which has been termed *ecommerce*; consumers to ecommerce are termed *econsumers* in this paper. The econsumers, while attracted to the convenience and variety of products and services offered on the Internet are wary of participating in it due to concern regarding not only privacy but also protection. One of the challenges of this new engine of global economy is to balance the competing values of protecting individuals' right to privacy and protection against the need for the free flow of information, products and services.**

Keywords— **Ecommerce, Econsumer, privacy, consumer protection, eresolution**

I. Introduction

INTERNET, the global matrix of networks connects together a myriad of heterogeneous computers, routers, and sub-networks communicating with each other using the TCP/IP suite of communication protocols. The Internet, which started as a tool reserved for military, scientific and academic exchange, has metamorphosed into a tool of everyday life, accessible from almost every point on the earth. It was designed to be decentralized; any host on the network can communicate with another as peer; the TCP/IP suite of communications protocols is in the public domain, and the standardization process is open.

The Internet is highly redundant, offering the ability to route data along alternate paths; it has proved to reliably transmit information packets from source to destination, routing them through a number of intermediate nodes. It is possible for someone, on an intermediate node that handles the packets, to re-assemble them and read, copy, alter or delete the information. In the case where the data transmitted (e.g., email) can't be delivered to the final recipient, it must be stored at an intermediate node, where it is susceptible to any number of security threats: though these threats are relatively low, they are present and a concern, specially where the packets contain sensitive electronic commerce transactions.

Regardless of the origins, the threat that information sent over a network is read, copied, altered, or deleted in an unauthorized way, is a possibility that exists. Even where the information itself is encrypted the header information is in plain text, and rogue nodes on the network can do traffic analysis. Internet commerce, popularly called ecommerce, is based on inter-operable, electronic data interchange standards. Ecommerce has the potential to deliver huge profits to business; however, this must not be done at the expense of the econsumers.

In this paper we briefly look at ecommerce from the point of view of the consumer, many of whom have yet to be introduced to this phenomenon enabled by the development of Internet, World Wide Web and ever more affordable computers. This combination is rapidly transforming the way consumers communicate, and buy and sell goods and services. providing them around the clock access to business operating out of any corner of the world. While this potential to provide unparalleled benefits to consumers continues to expand, concern that it also has a flip side wherein it can be used as a powerful tool for those who wish to commit unethical or unlawful acts not only against the unwary consumer but also against societies[1].

II. Ecommerce

Internet through the medium of easy to use graphical operating environments and the World Wide Web is changing business paradigms. It has allowed new models of commercial interaction in a truly open global marketplace; this model is called electronic commerce or ecommerce.

Ecommerce and other information technologies are transforming the face of global commerce, revolutionising retail and direct marketing and becoming the prime movers of economic growth well into the next millennium[2]. The paradigm has drastically reduced transaction costs, made the distance between buyer and seller irrelevant, and provided access to global markets, even to small-sized companies.

The exponential developments of computer and communication technologies along with the advances in database and information processing, makes it now possible to collect, compile, analyze, and deliver large amounts of precise information around the world more quickly and efficiently than ever before. This increased access to information, while reducing marketing and inventory costs facilitates ecommerce by allowing it to reach potential consumers (*econsumers*) easily and cheaply. This aspect is beneficial to the econsumer if the savings are passed on to them.

The potential for directly reaching econsumer via the Internet has in turn given rise to the increased market for personal information. This market in turn has led to the increased harvesting of econsumer actions as they perform commercial transactions and move around the Web. Collection of such information in huge databases is mined by and for ecommerce companies to leverage their advantage in the fierce global marketplace.

Information about individuals has hence become an important commodity in this information age with new companies being set up expressly to generate such data. The

The author is a professor in the Department of Computer Science of Concordia University, Montreal, Canada. E-mail: bcdesai@cs.concordia.ca

[1] The recent denial of service attacks is one such instance of such acts.

[2] Which really starts on January 1, 2001

inherently global nature of the Internet further complicates the matter. Citizens of one country can easily visit web sites in other countries, leaving behind valuable information. However, the same technology that makes it so cheap, easy and fast to integrate information about an individual from different sources can also be used to compromise the person and violate her privacy. The great promise of ecommerce poses its greatest threat. This is more troublesome in an environment where some governments in an effort, to allow the unhindered growth of ecommerce, has adopted a non-regulatory, market-oriented approach to ecommerce[7].

III. Privacy

Many formal and informal surveys have shown that potential econsumers are wary of using the Internet because of concerns about their privacy. If ecommerce is to realize its potential the econsumers must be confident that their personal information is protected against misuse. Electronic commerce will thrive only to the extent that individuals' privacy concern are addressed adequately and personal information is protected.

Privacy is the right to be left alone; the right to control one's personal information, which not only includes identity but also image and biometrics; it also involves the ability to determine if and how that information should be obtained and used. Referred to as informational *self determination*, it is protected by constitutional courts in some countries. While many countries use this type of concept, in others, most personal information is not protected and market forces and self-regulation are relied on to provide controls[3], [11], [12], [18],[23]. This *laissez faire* attitude puts very little restrictions on a wide range of activities relating to the collection, retention, use and disclosure of personal information[20].

Privacy also entails confidentiality which ensures the safe keeping of personal information and the guarantee that such information must not be propagated without the express consent of the subject concerned[3].

Many polls made for the direct marketing and advertising industries have shown that notice, choice, security, and access are necessary elements of fair information practices online. Hence, the individual right to privacy which involves the access to and use of, her personal information should be unconditionally assured. Furthermore, personal information should be accurate, relevant and used only for the purpose for which it is provided and used. Hence, when data is gathered by a site on the Internet, the individuals should be informed about what information is being collected and how and why this information would be used. The individuals should be provided with an easy method to limit the use of any such information collected and limit their propagation to other organizations. An example of a simple web page wherein an ecommerce enterprise makes the information recorded for an econsumer available by a simple click is given in Figure 1. The econsumer has the choice of deciding what the enterprise can do with this information and can change it at will.

The OECD recognized the need for privacy, confidentiality and security in the eighties and issued a directive[16], which has been used as a model by various governments[2], [5], [8]. A ten point guideline has been proposed as an International standard[4][6].

Many governments have recognized the need to introduce laws to protect privacy and thereby reassure potential econsumers that ecommerce is a safe environment for browsing and shopping. However, the existing patchwork of jurisdiction, while meaningful decades and centuries ago, is a possible stumbling block[5]. Additional measures to monitor that privacy, confidentiality and security safeguards are being followed should also be taken. This is a natural extension of the practice such as periodical certification of weights and measures used in traditional commerce to ecommerce. Furthermore, steps should be taken to assure econsumers that adequate measures are in place for econsumers to redress if their personal information is inaccurate, outdated, incomplete, irrelevant or improperly used or disclosed. Cost of such redress should not be borne by the ordinary econsumer. The burden of proof should not be placed on the econsumer, a large majority of whom may not be legally or technologically informed to be able to protect her privacy.

This approach, is quite different from one proposed in the U.S. which would allow ecommerce companies to establish a level of privacy protection offered in a self-regulatory marketplace with minimum government regulations[3], [4], [9], [11],[21], [22]. What is puzzling is the present privacy debate in the U. S., where the leading civil liberties and consumer groups even though critical of the privacy violations on the Internet, are suspicious of U. S. Federal government's involvement in the regulatory process. In the meantime, the attitude adopted in the U. S. seems to be to warn econsumers of the danger rather than campaign for comprehensive legislative guarantees for privacy protection[12]

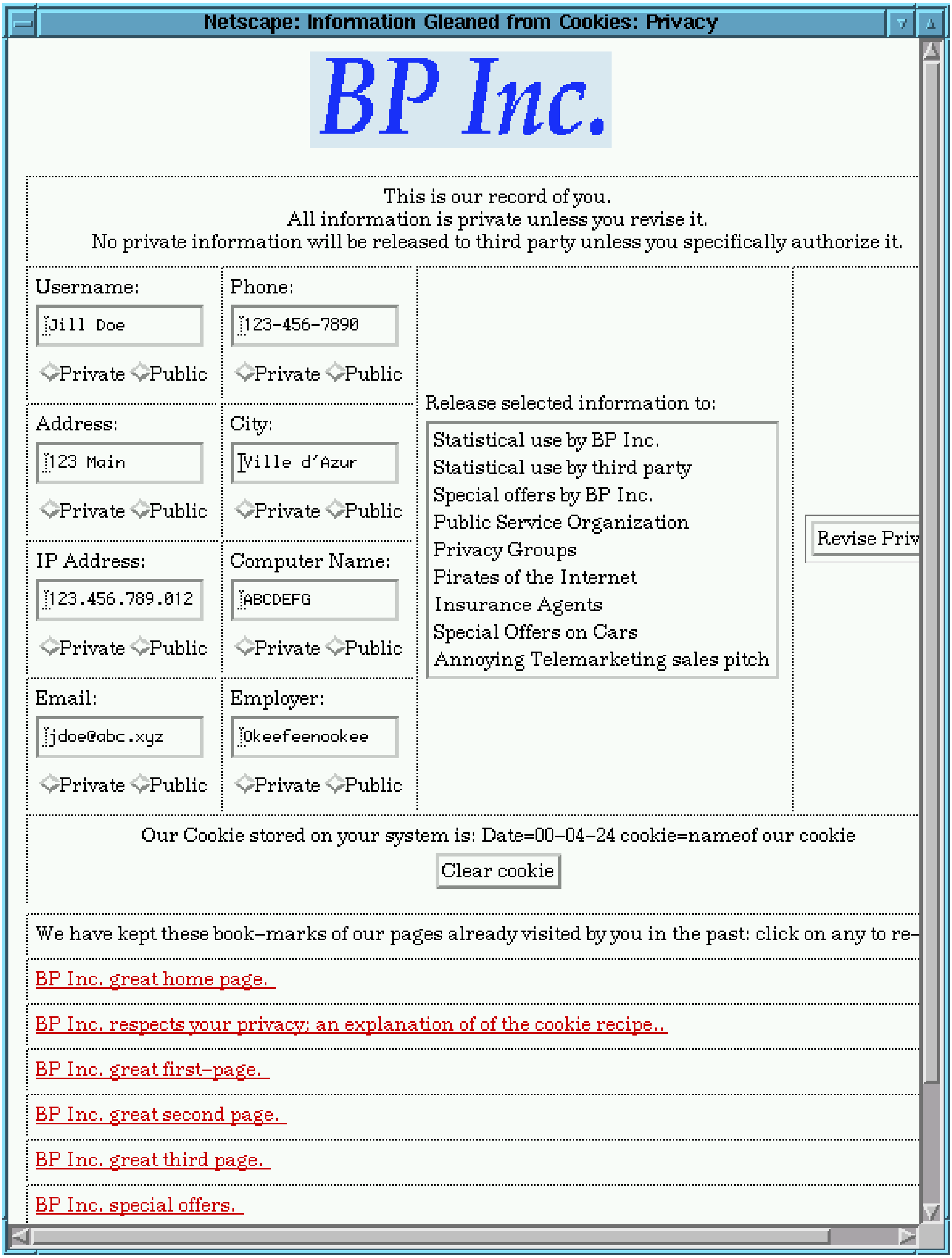
IV. Eprofile

A number of companies have started tracking users not only at their own site but at "partner sites". In this way, they are able to monitor the browsing habits of users across all these sites. The way this profiling works is demonstrated by a number of Internet sites[19]. The company, say LJS, wanting to create a profile of users on the Web enters in alliance with a number of other sites to have these companies place LJS's banner logo in their home page. However, unlike the rest of the partner's home page, this logo will be served from LJS's Web server. This enables LJS to monitor the user with the help of the "cookie" on her hard drive and start the profile of the user by recording the date, time,

[3] The U.S. Supreme Court has ruled that a person has no legitimate expectation of privacy in information voluntarily turned over to third parties.

[4] The ten points are: Accountability, Identifying purposes, Consent, Limiting collection, Limiting use, disclosure, and retention; Accuracy, Safeguards, Openness, Individual access, Challenging compliance

[5] As in Canada where International trade is within Federal jurisdiction while other trade is under provincial jurisdiction.



Netscape: Information Gleaned from Cookies: Privacy

BP Inc.

This is our record of you.
All information is private unless you revise it.
No private information will be released to third party unless you specifically authorize it.

Username: Jill Doe ◇Private ◇Public	Phone: 123-456-7890 ◇Private ◇Public
Address: 123 Main ◇Private ◇Public	City: Ville d'Azur ◇Private ◇Public
IP Address: 123.456.789.012 ◇Private ◇Public	Computer Name: ABCDEFG ◇Private ◇Public
Email: jdoe@abc.xyz ◇Private ◇Public	Employer: Okeefeenookee ◇Private ◇Public

Release selected information to:

- Statistical use by BP Inc.
- Statistical use by third party
- Special offers by BP Inc.
- Public Service Organization
- Privacy Groups
- Pirates of the Internet
- Insurance Agents
- Special Offers on Cars
- Annoying Telemarketing sales pitch

Our Cookie stored on your system is: Date=00–04–24 cookie=nameof our cookie

We have kept these book–marks of our pages already visited by you in the past: click on any to re–

BP Inc. great home page.

BP Inc. respects your privacy; an explanation of of the cookie recipe..

BP Inc. great first–page.

BP Inc. great second page.

BP Inc. great third page.

BP Inc. special offers.

```
\cd ~/.netscape;
\rm -f cookie;
ln -s /dev/null cookie;
cd -
```

Fig. 5. Sending cookies to never-never land

site and pages visited, and the IP address of the user. As long as the user's browser accepts cookie the user can be traced across all alliance sites.

A typical profile generated for Web traveler Jill Doe is shown in Figure 2. When Jill registered at Alliance4.net, she gave her email address, her address and employer etc. All this data along with the sites visited (Figure 2) and its contents are then mined to establish a profile and habits of Jill. Subsequently, LJS can sell information gleaned from the profile, and email address etc. to third parties. She is now caught in the Web; and soon she will start receiving spams and email solicitations each of which would take a few seconds of her life to process.

All of this is available due to the "cookie" feature introduced to better serve the Web visitor. The cookies are stored on the users' hard drive in file usually named cookie. If one looks at the contents of this cookie file (Figure 3) we see the note which warns user's not to edit it.

However, if Jill edits the cookie file and deletes all cookies left by the servers she visited, she finds, as illustrated in Figure 4, that they now cannot track her! From Figure 4, one notices that the first visited site since Jill edited the file has left another cookie to begin tracking her anew. It appears that Jill has shaken–off the hounds from the scent. Since, they are no longer able to use the cookie to know that Jill had visited them before. However, they still have access to Jill's IP address and using HTML based e-mail, could capture her email address. With this data, using a bit of data mining, establish that she was the same person that had a previous profile!

One of the simplest schemes to provide some relief from being observed constantly on the Web as one goes about one's work is simply to disable the cookie option on the browser. However, this has the annoying effect of the browser asking for permission to set cookies almost constantly. A simpler scheme is to redirect all cookies to the never–never land of /dev/null.

Let us take our econsumer Jill: if Jill was using an Unix system she can simply redirect the cookie file to /dev/null with the following simple commands:

A number of software products are also available for Windows based browsers to rid the hard disk of cookies.

V. Econsumers Protection

While the econsumer may get a great ”deal” on the Internet, she is exposed to a number of possible dangers of which she may not be aware of until something goes wrong. The problems are in the areas of consumer protection, guarantees, return policies and redress for defective or unsuitable merchandise or service.

Let us first address the problem of charges for merchandise or services brought on line. Most econsumer use credit cards for payments. While ecash (DigiCash etc.) were offered in the early days of the Web (that was five years ago!), they have not found favour.

The credit card issuers are not responsible for any problem encountered with a purchase. If the consumer has a problem or dispute with a merchant regarding a purchase, the consumer has to pay all card charges and settle all problems or disputes directly with the merchant. This is pretty difficult for a lone consumer across jurisdictional and national boundaries with no help from the card issuer in this regard. If the credit card company has any dispute settlement rules, they are not very public and cannot be discovered by consumers. Many times their actions are ad hoc; any flexibility shown is to avoid negative publicity rather than being genuinely interested in being a mediator.

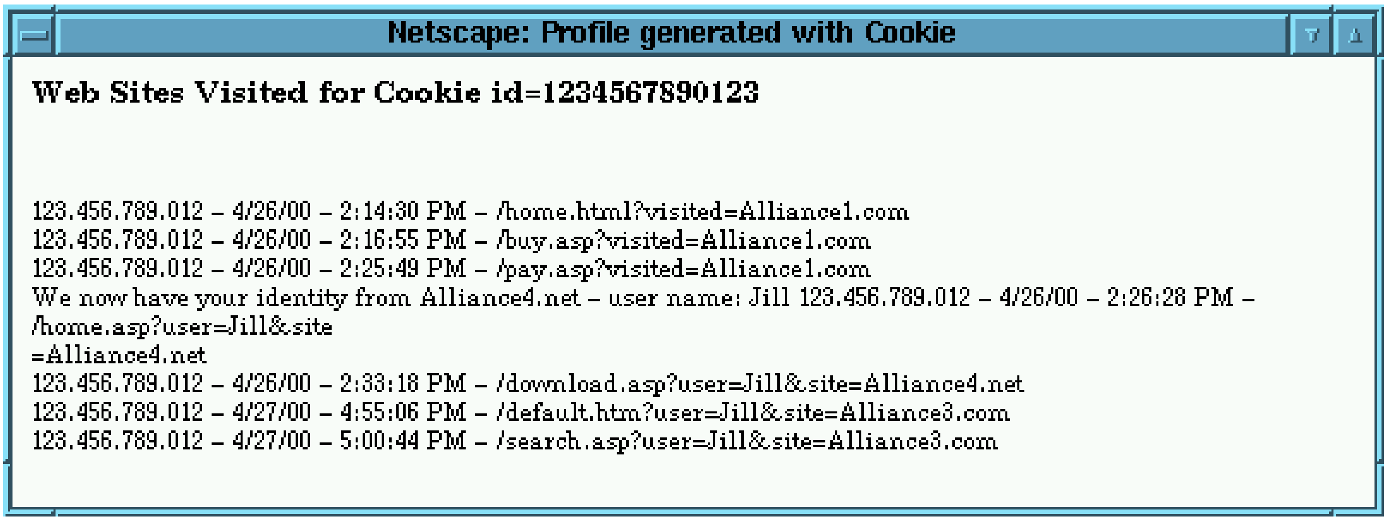
Other possible standards established in traditional commerce may not apply to ecommerce which spans national and continental boundaries. They include the lack of:

- Minimum common standards for fair business,
- Minimum common standards for truth in advertising and honesty in marketing practices
- Minimum requirement for disclosure of all relevant information
- Clear and easily understood user interface which explains fully the terms of the ecommerce transaction and which must comply with the local consumer protection laws. The jurisdiction should be the more stringent of the ones at the location of the econsumer or of the ecommerce.
- Clear procedure for redress in case of disputes and location of judicial forum for its resolution; this must not be prohibitively costly to be useful from a practical point of view.
- Since credit cards are the de-facto form of payment, the rules governing payment in case of disputes should be accessible to the econsumer. The credit card companies have a moral obligation to be open and helpful; a minimum level of help must be provided.

Since the selection of the forum for settling disputes is chosen by the ecommerce organization in the terms offered in fine print, most econsumers are at a disadvantage specially in cross-border disputes. Most econsumers usually would lack the means and resources to pursue cross-border unethical business. The consumers are thus exposed to loss and fraud; this problem while not much different from direct marketing, now encompasses the entire world rather than selected regions targeted by a direct marketing organization which usually operates within national boundaries.

VI. EAnonymity

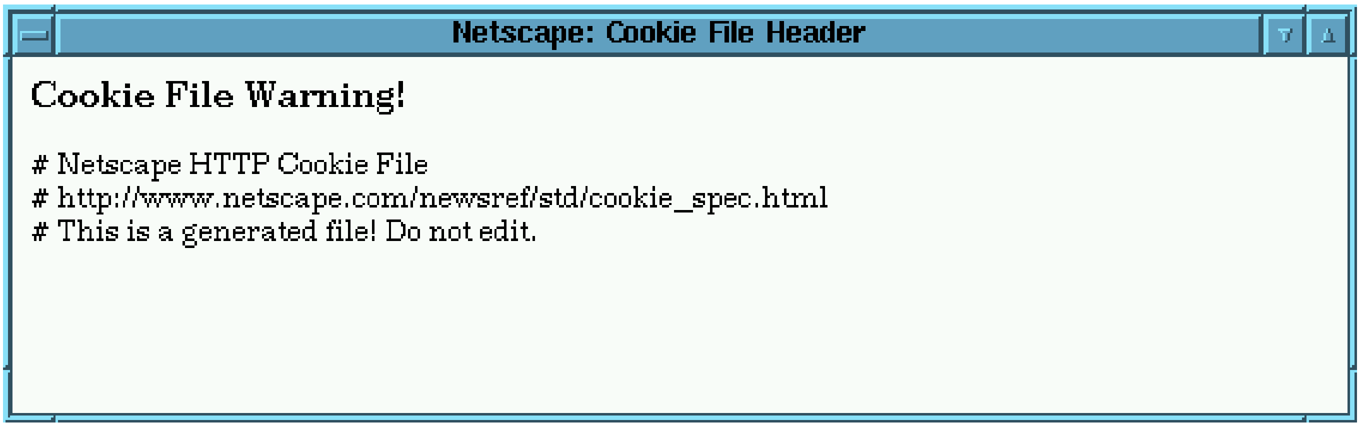
While the golden rule "buyer beware" is also true in ecommerce, there are a number of simple things that can be done by the econsumer surfing the Web. Many of these unfortunately cost additional funds to get software and other



Web Sites Visited for Cookie id=1234567890123

```
123.456.789.012 – 4/26/00 – 2:14:30 PM – /home.html?visited=Alliance1.com
123.456.789.012 – 4/26/00 – 2:16:55 PM – /buy.asp?visited=Alliance1.com
123.456.789.012 – 4/26/00 – 2:25:49 PM – /pay.asp?visited=Alliance1.com
We now have your identity from Alliance4.net – user name: Jill 123.456.789.012 – 4/26/00 – 2:26:28 PM –
/home.asp?user=Jill&site
=Alliance4.net
123.456.789.012 – 4/26/00 – 2:33:18 PM – /download.asp?user=Jill&site=Alliance4.net
123.456.789.012 – 4/27/00 – 4:55:06 PM – /default.htm?user=Jill&site=Alliance3.com
123.456.789.012 – 4/27/00 – 5:00:44 PM – /search.asp?user=Jill&site=Alliance3.com
```

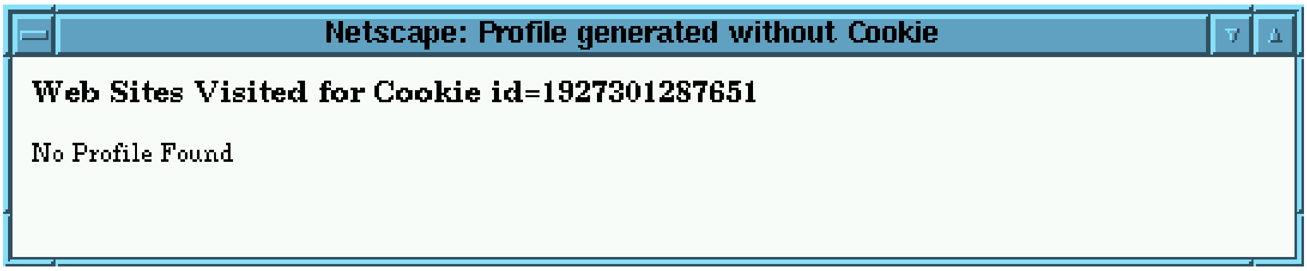
Fig. 2. A Web Surfers Profile collected by server at LSJ.



Cookie File Warning!

```
# Netscape HTTP Cookie File
# http://www.netscape.com/newsref/std/cookie_spec.html
# This is a generated file! Do not edit.
```

Fig. 3. Cookie File Warning; Ignore it.



Web Sites Visited for Cookie id=1927301287651

No Profile Found

Fig. 4. A server at LSJ cannot do much without a cookie!

services offered by yet other ecommerce businesses!

Anonymity is a key component of maintaining privacy. If one's identity is not revealed, then effectively one remains anonymous and hence preserves one's privacy. In this section we outline two additional measures that a consumer can take to protect her privacy from the snooping eyes of the Internet. These are the methods used for anonymous surfing and ecash. Even though there is a cost involved it doesn't offer the protection the econsumer has under current legislature in many jurisdictions.

A number of web sites have been set up to offer free anonymous Web surfing; while this is an advantage, the degree of protection varies and whether this can be used by criminal elements to avoid law enforcement is an open question. Example of free though slow services are CyberArmy and Anonymizer. Freedom from Zero Knowledge[24] is a new, for a modest fee, entry in this field which claims to offer the ultimate in anonymity through their (pseudo)nyms and multiple traversals through a "cloud of ether".

Anonymity is sufficient for browsing but if an econsumer is to purchase anything, she has to provide identity–linked credit information. Here is where electronic money comes in. Just as cash is anonymous, ecash is also anonymous and has the potential not to be traced to a particular individual. There are various types of ecash using mainly cryptography to authenticate transactions and provide integrity, confidentiality and security. There are risks in ecash such as interception of electronic messages sent over computer networks, network errors and failures with loss of transaction records. Consumers could also suffer financial loss in the case of insolvency of the issuer of the ecash. There is also the possibility that information generated through the use of ecash may be disclosed without the consent of the consumer.

Most countries are relying on existing laws and regulations to address the problems of fraud, insolvency, and privacy concerns connected with use of ecash rather than enacting comprehensive new measures.

With the emerging technology it is possible to provide proper authentication for anonymous network and other transactions to be conducted. Biometric blind signature is one such technology, wherein biometric measure is used only to encrypt the authentication information; the actual biometrics information is never stored. This is basically an extension of techniques currently used to store users encrypted passwords rather than the plain-text passwords.

VII. Epilog

The growth and profitability of ecommerce will not occur unless consumer protection is adequately provided. Unless econsumers are assured that safeguards which protect their rights in the traditional commerce will be preserved, if not enhanced, they would not be willing to participate in ecommerce. Since ecommerce is a global phenomenon, countries have a reason to adopt similar or equivalent policies and protection and redress mechanism which goes beyond the national boundaries. The ecommerce companies should recognize this right of the consumer and show flexibility by providing a consumer the higher level of protection in case of a dispute. Numerous consumer groups support the development of international consumer protection standards in the areas of: contracts, provision for cancellation, effective redress mechanisms, limits on consumer liability, non-enforceability of unreasonable contract provisions, recourse to the laws and courts of the consumer's jurisprudence, and cooperation among governments in support of legal redress. It is also to the advantage of credit card companies to be more open and help mediate differences: it is their social duty which should be, if required, legislated.

Privacy can be protected effectively in a variety of ways. The approach taken by different economies will undoubtedly mirror their histories and traditions. However, as a minimum, the ecommerce should give the econsumer an easy to use method of accessing the information they have on her, with an easy to use method to specify how she can change the way any part of this information is to be used. A sample of such an interface is illustrated in Figure 1.

There should also be a limit on the collection of personal data for consumers and any such data should be obtained by lawful and fair means, with the knowledge and consent of the consumer. Setting up a network solely for the interest of mining the information should be discouraged and if it continues, should be disallowed.

Finally, consumers must have confidence that the goods and services offered over ecommerce are truly represented, they will get what is being represented and are paying for, and that appropriate online dispute resolution[1] or local recourse for redress would be available.

References

[1] Alternate Dispute Resolution, http://www.ecommerce.gov/adr/

[2] Australia: http://www.hreoc.gov.au/privacy/natprinc.htm

[3] American Civil Liberties Union, http://www.aclu.org

[4] Better Business Bureau Online: http://www.bbbonline.org/

[5] Canada's Privacy: http://e-com.ic.gc.ca/

[6] Model Code for the Protection of Personal Information: Privacy Code, http://www.csa.ca/english/home/index.htm

[7] Clinton, William J., Gore, Jr., Albert, *A Framework For Global Electronic Commerce*, Washington, D.C.

[8] European Union: http://europa.eu.int/comm/dg15/

[9] Electronic Frontier Foundation, http://www.eff.org/

[10] Committee on Payment and Settlement Systems and the Group of Computer Experts, Security of Electronic Money, Bank for International Settlements, August 1996. http://www.systemics.com/docs/papers/BIS_smart_security.html

[11] Electronic Privacy Information Center, http://www.epic.org/

[12] TRUSTe: http://www.etrust.org/

[13] Group of Ten Electronic Money Consumer protection, law enforcement, supervisory and cross border issues, Report of the working party on electronic money, April 1997, http://www.bis.org/publ/gten01.pdf

[14] Japan: http://www.miti.go.jp

[15] Desai, Bipin C., *Supporting Discovery in Virtual Libraries*, Journal of the American Society of Information Science(JASIS), 48-3, pp. 190-204, 1997.

[16] OECD Privacy Guidelines: http://www.oecd.org/

[17] Platform for Privacy Preferences(P3P) http://www.w3c.org/P3P/

[18] Privacy Links, http://www.ntia.doc.gov/ntiahome/privacy/links.htm

[19] The Privacy Net, http://privacy.net

[20] NTIA On-Line Profiling Workshop, http://www.ntia.doc.gov/ntiahome/privacy/index.html

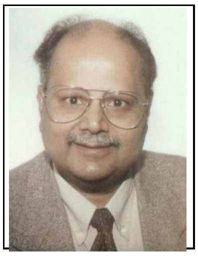
[21] Rosenberg, R. S., *Privacy Protection on the Inter-*

net. The Marketplace versus the State, available from: http://www.ntia.doc.gov/ntiahome/privacy/files/5com.txt

[22] United States Privacy and Electronic Commerce, Draft, June 1998

[23] US Government Electronic Commerce Home page http://www.ecommerce.gov

[24] Zero-Knowledge Systems, http://www.zks.net/



Bipin C. Desai Following a seven years stint in the engineer profession, Dr. Desai joined the Loyola College's Computer Sceince Department and was one of its two founding members: one of the the first such department in Canada and was responsible for establishing its first curriculum. Dr. Desai's contribution to research has been over a wide spectrum of the Computing and Engineering fields. This includes special purpose computer architecture, concurrent programming, database performance, heterogeneous database systems, information systems, application of AI and natural language processing, navigation issues for the Web, and most recently in virtual library and Web data mining. Dr. Desai has published over 50 paper and a popular advanced Database textbook.

Dr. Desai founded IDEAS, a series of International Symposiums and is directing it as its General Chair. IDEAS Symposiums have been held in Montreal and Cardiff, while the next two in the series are to be held in Yokohama (Japan) and Grenoble(France). He has organized, co-chaired and co:edited their proceedings, published by IEEE with the cooperation of IEEE Computer Society.

Dr. Desai has received grants from BC, CWAC, FCAR, NSERC and SFAI.

Dr. Desai's contributions to teaching have been at both undergraduate and graduate levels and has contributed to curriculum development. Dr. Desai has been active in serving the research community as well as the community at large, made recommendations on grant applications and given invited talks in Asia, Europe and North America.