Research Paper
Impact Factor: 3.996
Peer Reviewed & Indexed Journal

IJMSRR
E- ISSN - 2349-6746
ISSN -2349-6738

ONLINE ADVERTISING AND HIDDEN HAZARDS TO CONSUMER SECURITY AND DATA PRIVACY IN WORLD SCENARIO

V.Thanigairajan* Dr.R.P.Ramesh**
**Head - Department of Commerce, Bharathidasan University Model College, Thiruthuraipoondi.*
***Assistant Professor,Rajah Serfoji Govt Arts College (Autonomous), Thanjavur.*

Abstract
With the emergence of the Internet and e-commerce, more and more commonplace activities are taking place on the Internet, which has led to major advances in convenience, consumer choice, and economic growth. These advances have also presented novel questions concerning whether consumer security and privacy can be maintained in the new technology-based world. We will examine these issues today specifically in the context of online advertising, where vast data is collected and cyber criminals exploit vulnerabilities in the system and use malware to harm consumers. Consumers who venture into the online world should not have to know more than cyber criminals about technology and the Internet in order to stay safe. Instead, sophisticated online advertising companies like Google and Yahoo! have a responsibility to help protect consumers from the potentially harmful effects of the advertisements they deliver.

Keyword: Online advertising, E-Commerce, Spyware, Cookies, Malware.

Online advertising and privacy risk.

An overwhelming majority of consumers are less likely to click on online ads because of privacy concerns, according to a report. Levels of concern over online privacy are growing, according to a report by data privacy consultants TrustE. Eighty-nine per cent of British consumers are worried about data privacy, the report found, with 60 per cent of those people saying they are more concerned than they were a year ago.

Of those reporting greater concern, almost two-thirds (60 percent) said companies sharing personal data with other companies were the cause of their worry. More than half (54 percent) said brands using data to serve behavioral ads to them was the reason they were more concerned.

Despite headlines about US intelligence services' surveillance of people's personal information in 2015, only 20 per cent said such stories were the reason for their increased concern.

The increasing level of concern does not appear to be without consequence. Ninety-one per cent are less likely to click on online advertisements, while 78 per cent said they would avoid using Smartphone apps if they believe the company does not protect their privacy.

Ken Parnham, European managing director of TrustE, says: "Lack of trust can starve businesses of valuable data and sales, restricting the lifeblood of the digital economy as people are less likely to click on ads, use apps or enable location tracking on their smart phones.

"These findings show that success is no longer just about innovation, companies need to take decisive action to address online privacy concerns to stay ahead of the competition, minimize risk and build online trust."

Consumers' awareness about privacy risk of online advertising.

At present in the era of technological revolution consumers are familiar in online advertising but their knowledge about risk of privacy is not satisfactory Consumers don't always understand how behavioral advertising works and, in the absence of information, many will assume that the data activities are more privacy invasive than what typically occurs behind the scenes. For example, more than 1 in 3 consumers believe that websites share their contact information (email, phone number etc.) or name with advertisers without their consent. In reality, most behavioral advertising operations only know consumers by anonymous cookies, not name. When consumers assume the worst it can profoundly affect how they feel about behavioral advertising. In 2013 a survey conducted by the powering privacy compliance, risk management trust reveals 56% of consumers are concerned that when they use online advertising their personal information is being shared with others without their permission.

Further the research found that only 37% of consumers know how to protect their personal information online and consistently take the necessary steps to do so. Only 25% indicated that they regularly opt-out of online tracking, but the consumers opt-out at far lower percentages. And it is observed that the paradox between consumer privacy opinions and privacy actions, but this should not lead us to conclude that consumer don't actually care about privacy. A consumer's

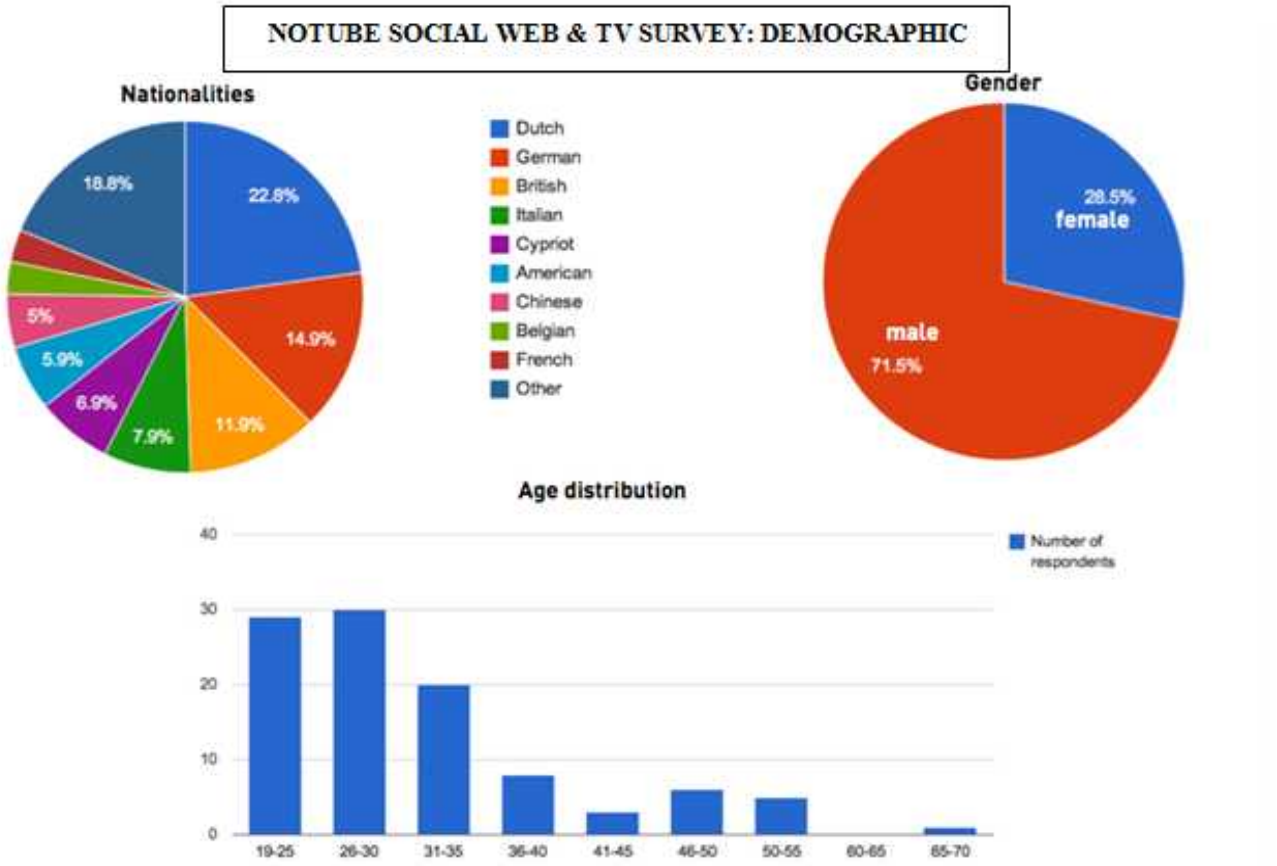
privacy perception about a website or platform can substantially alter the way that they interact with it. The significant, consistent lift and ROI our clients experience when displaying our privacy seal is proof of this. Better privacy creates more consumer trust, which leads to increased interactions and openness.

A new perspective on data privacy

The results of a recent survey of consumers and executives show that consumers have a keen sense of awareness of the risks surrounding data security and privacy, and that many consumer product executives are likely overestimating the extent to which they are meeting consumer expectations related to data privacy and security. On the other hand, many consumer product executives may be underestimating the opportunity for competitive advantage associated with meeting consumer expectations regarding data privacy and security. Furthermore, many consumer product companies do not seem positioned to gain consumer trust based on their current data privacy and security strategies, policies, and systems. The field appears wide open for consumer product companies to differentiate themselves through a reputation for strong data privacy and security practices. Consumer product executives should consider viewing data privacy and security not just as a risk management issue, but as a potential source of competitive advantage that may be a central component of brand-building and corporate reputation.

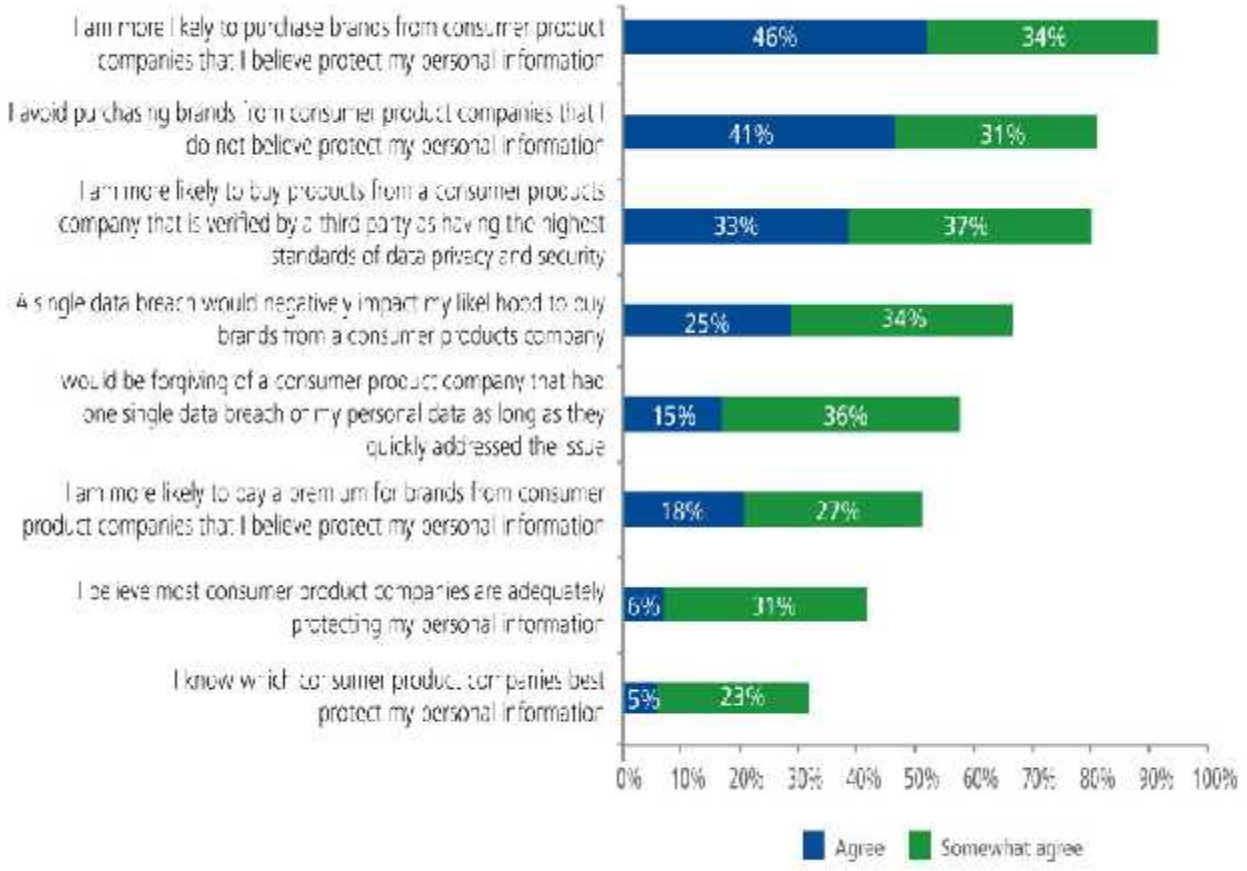
Data privacy and security as a competitive advantage

A broad survey conducted by the notube social web tv in throughout the world. The details of the participants are given bellow.



There is a clear connection between consumers' perceptions of data privacy and security practices and commercial success. Half of the consumers surveyed "definitely consider" the privacy and security of their personal information when choosing an online retailer, and 80 percent say they are more likely to purchase from consumer product companies that they believe protect their personal information. Furthermore, 70 percent of consumers would be more likely to buy from a consumer product company that was verified by a third party as having the highest standards of data privacy and security. In short, strong data privacy and security practices are not just about risk mitigation, but also a potential source of competitive advantage.

Figure 3. Consumers' attitudes and behaviors toward data privacy and security



Source: Consumer responses from the consumer product consumer and executive survey on data privacy and security, Deloitte LLP, August 2014.

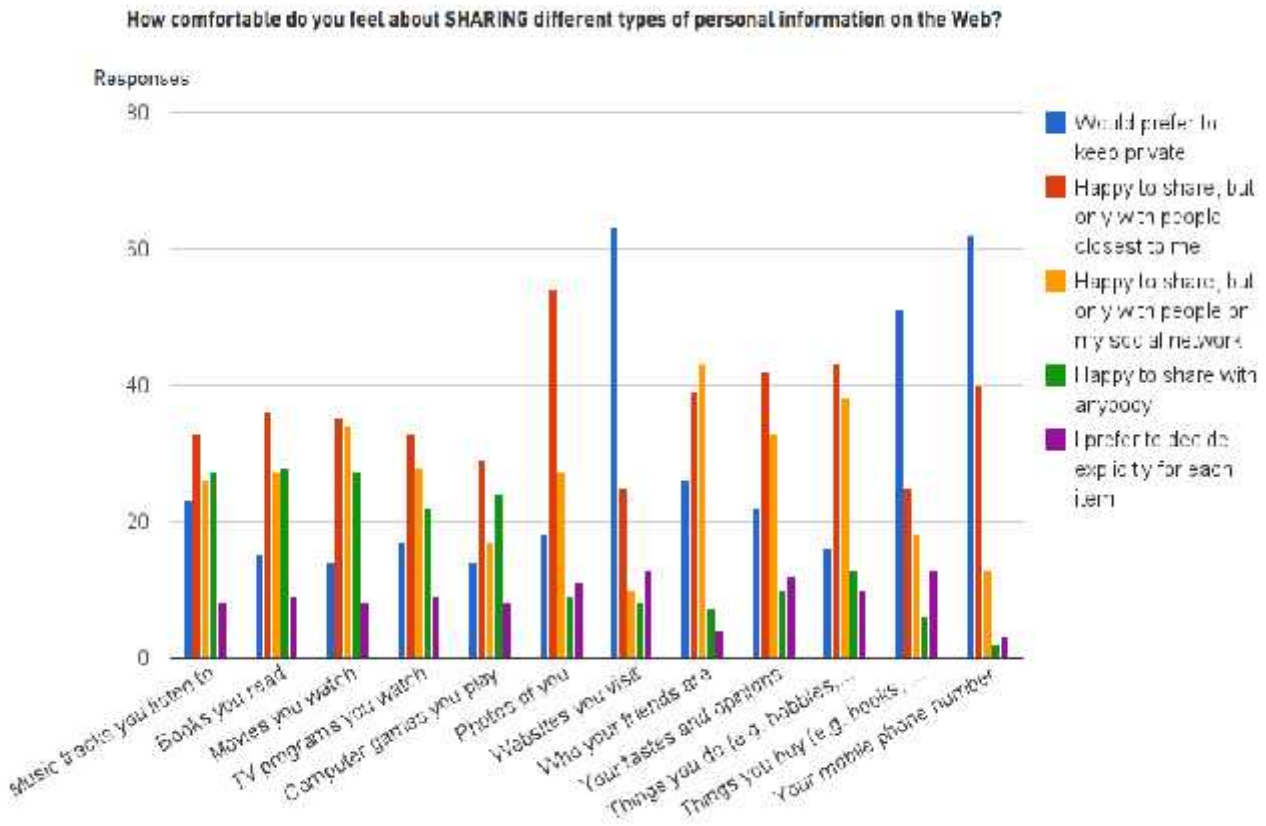
Graphic: Deloitte University Press | DUPress.com

The survey suggests that the field is wide open for consumer product companies to build a reputation for strong data privacy and security practices. Today, few consumers (37 percent) believe that most consumer product companies are adequately protecting their personal information. Even fewer consumers (28 percent) think that they know which consumer product companies best protect their personal information. These findings suggest that consumer product companies have yet to establish a name for themselves as trusted stewards of consumer data—and that a company in the industry that can do so can set itself apart from the competition.

Privacy is still an issue and consumers want to feel in control of their own data

In general people still feel relatively cautious about sharing *their own* activity and preference data on the Web:

- 74% of the sample *disagreed* with the statement that disclosing their data online is 'not a big issue' for them.
- Whilst they are willing to share data about most of the things they do online (their activity data), as shown in the graph below, their preference is to share it only with those closest to them – i.e. their friends and family, not with everyone – *or even with everyone in their social networks*, as is the case with the current trend for frictionless sharing.
- There is a strong reported preference for a high level of control over personal data: 94% agreed or strongly agreed with the statement "I want to be able to delete specific activities and preferences", and 73% with the statement "I want to keep certain programmes I watch private".



These results validate many of the assumptions behind the design of the Bean counter user interface, which keeps all data private by default, allows you to delete specific activities, and allows you to delete or hide specific interests. We felt these features were important to help protect users from inadvertently making public potentially sensitive or incorrect information that might emerge when previously disconnected pieces of personal data are combined and analyzed for patterns.

The results are also consistent with initial findings of some recent BBC user testing for the European Future Internet research project. Participants in the study also said they wanted control over their data, even though the perceived privacy risks associated with the data (the BBC programmes they had watched on TV) were relatively low and the perceived benefits, in terms of examples of more personalized future TV services, were relatively high.

How Online Advertisers May Steal web surfers Personal Information: Recommendations for Protecting Consumers.
So many experts are do research in this area and present their findings and recommendation after go through all of them some points are uniformly noted by everyone their research they are as follows.

Findings

1. **Consumers risk exposure to malware through everyday activity.** Consumers can incur malware attacks by simply visiting even a mainstream website and without taking any action such as clicking an advertisement. The complexity of online advertising makes it impossible for consumers to avoid advertising malware attacks or identify the source of the malware exposure and determine whether the ad network or host website could have prevented the attack.

2. **The complexity of current online advertising practices impedes industry accountability for malware attacks.** The online advertising industry has grown in complexity to the point that each party can conceivably disclaim responsibility when malware is delivered to a user's computer through an advertisement. Due to the many layers of intermediaries through which online advertisements often travel before appearing in a user's browser, the

ad networks themselves rarely deliver the actual advertisement from their own servers and the owners of the host website visited by a user often does not know what advertisements will be shown on their site.

3. **Self-regulatory bodies alone have not been adequate to ensure consumer security online.** Self-regulatory codes of conduct in online advertising do not fully address consumer security from malware. Interestingly, self-regulatory efforts in online security to date have been dependent on online ad networks for funding and viability, which creates a potential conflict of interest in their dual roles as industry advocates and standard-setting bodies.

4. **Visits to mainstream websites can expose consumers to hundreds of unknown and potentially dangerous third parties.** Even visiting a mainstream website exposes consumers to hundreds of third parties, and each of those third parties may be capable of collecting information on the consumer and may be a potential source of malware.

5. **Consumer safeguards are currently inadequate to protect against online advertising abuses, including malware, invasive cookies, and inappropriate data collection.** Self-regulatory codes do not significantly address online advertising security and data collection protections are often limited in scope and underutilized. Current FTC safeguards are insufficient to protect consumers from online advertising abuses, and cybercriminals are constantly finding new ways to evade existing security methods.

6. **Current systems may not create sufficient incentives for online advertising participants to prevent consumer abuses.** Due to the difficulty in determining responsibility for malware attacks and inappropriate data collection through online advertisements, online advertising participants may not be fully incentivized to establish effective consumer safeguards against abuses.

Recommendations

To remedy the problems identified above, the Senate Subcommittee proposed four recommendations to tighten online advertising protocols and protect consumers.

1. **Establish better practices and clearer rules to prevent online advertising abuses.** Currently, legal responsibility for damages caused through malvertising usually rests only with the fraudulent actor in question. Since these actors are rarely caught and even less frequently able to pay damages, the harm caused is often borne by consumers. Sophisticated commercials entities, large and small, should take steps to reduce system vulnerabilities in their advertising network, and if they fail to do so, then regulatory or legislative change may be needed to incentivize such entities to increase security for advertisements that run through their systems.

2. **Strengthen security information exchanges within the online advertising industry to prevent abuses.** Online advertising companies are often hesitant to share information regarding security hazards because of fears they will be accused of violating federal antitrust laws by cooperating with competitors. The Department of Justice and the FTC recently issued joint guidance suggesting that sharing of cyber threat-related information would not trigger antitrust liability and those agencies should clarify the extent to which online advertising participants may exchange information about security hazards. If necessary, Congress should pass legislation that removes legal impediments to the sharing of actionable cyber-threat related information and create incentives for the voluntary sharing of such information.

3. **Clarify specific prohibited practices in online advertising to prevent abuses and protect consumers.** Self-regulatory bodies should develop comprehensive security guidelines for preventing online advertising malware attacks. In the absence of such self-regulation, the FTC should consider stepping in and issuing regulations to prohibit unfair and deceptive online advertising practices. Greater specificity in prohibited or discouraged practices is needed before the overall security situation in online advertising can improve.

4. **Develop additional "circuit breakers" to protect consumers.** Given the complexity of online advertising, more "circuit breakers" should be incorporated into the online advertising system to introduce checkpoints and ensure that malicious advertisements are caught at an earlier stage before transmission to consumers.

Conclusion

Now a days a huge volume of business and economic activities are done followed by the online advertising, it is needless to say some greedy hackers bring into play with the personal data of online users it destroy the confidence of consumer to believe the privacy security. In online advertising due to little or no accountability for fraudulent actors and a lack of regulation in place to protect consumers against malicious online advertising. To safeguard the consumer's interest it is better

to establish an online monitoring mechanism by all over the world by the all country then only the eradication of online hackers and spyware and malware and other unethical activity is possible.

References

Books

1. Judy Strauss , Adel El-Ansary and Raymond Frost, " E-Marketing", Parson Education.
2. Avinash Kaushik, "The Art of Online Accountability & Science of Customer Centricity".
3. Roger C. Parker, "Streetwise Relationship Marketing On The Internet" . Adams Media Corporation.
4. J Suresh Reddy , "Impact of E-commerce on marketing", Indian Journal of Marketing. May 2003, vol xxxiii, No.5.
5. J Suresh Reddy , "Impact of E-commerce on marketing", Indian Journal of Marketing. May 2003, vol xxxiii, No.5.
6. Jaffrey Graham, "Web advertising's future >>> eMarketing strategy", February 28,2001

Websites

- http://web.ebscohost.com.
- http://customerworld.typepad.com/swami_weblog/2006/11/india_internet_.html.
- www.ascionline.org.
- http://www.newsandtech.com/issues/2006/03-06/ot/03-06_saxoonlineadseries-01.htm.
- http://www.easa-alliance.org/.
- http://webanalyticsindia.net/blog/2008/04/current-internet-status-and-webanalytics-oppurtunities-in-india/

Research papers and Articles

1. Abdul Azeem and Zia-ul-Haq (2012). "Perception towards Internet Advertising: A Study with Reference to Three Different Demographic Groups," *Global Business and Management Research: An International Journal*, Vol.4, No.1.
2. Jeffrey Parsons, Katherine Gallagher and K. Dale Foster, "Messages in the Medium : An Experimental Investigation of Web Advertising Effectivenessand Attitudes toward web Content" in Proceedings of the 33rd Hawaii International conference on system sciences – 2000 IEEE
3. Adeline Kok Li Ming, Teoh Boon Wai, Mazitah Hussin and Nik Kamariah Nik Mat (2013). "The Predictors of Attitude towards Online Advertising," *International Journal of Applied Psychology*, Vol.3, No.1.
4. Jean Louis Chandon, Mohamed Saber Chtourou , David R. Fortin, "Effects of Configuration and Exposure Levels on Responses to WebAdvertisements ", Journal of Advertising Research-June 2003.