Advances In Multidisciplinary & Scientific Research
A Multidisciplinary & Interdisciplinary Journal

Vol. 1, No. 1, June, 2015

Impact of Platform For Privacy Preference Developments On Ethical Issues

K.A. Bakare
Nigerian College of Aviation Technology, Zaria.
Aeronautical Telecommunication Engineering School, P.M.B. 1031,
Zaria, Kaduna State, Nigeria.
bakarre@yahoo.com

S.O. Yisah
Department of Mathematics,
Ahmadu Bello University, Zaria, Kaduna State, Nigeria.
yselinat@yahoo.com

Abstract
This paper reviews the effects of development of Platform for Privacy Preference (P3P) on ethical issues. P3P is a screening technology which helps shield users from sites that do not provide the level of privacy protection they desire. It discusses the evolution of P3P right from its inception up till the present time and its acceptance in the public. The findings showed that; though P3P could make privacy policies transparent but it cannot ensure that companies will follow privacy policies that have to do with ethical issues and this is the potential limitation of the work. The paper thereby recommends that implementation of P3P will lead to a greater openness, ethical conscious, more informed web users and greater accountability.
Keywords: Platform for Privacy Preference (P3P), privacy policies, web users and ethical conscious.

Aims Research Journal Reference Format:
K.A. Bakare & S.O. Yisah (2015): Impact of Platform For Privacy Preference Developments On Ethical Issues.
Aims Research Journal. Vol 1, No. 1 Pp 55 -60.

1. INTRODUCTION

Platform for Privacy Preferences (P3P) is a preference standard set by the World Wide Web Consortium (W3C), the main standard setting body of the web that serves as a potential solution to consumer privacy concerns. P3P is a screening technology which helps shield users from sites that do not provide the level of privacy protection they desire. Instead of forcing users to find and read through the privacy policy for each site they visit, Web browser software using the P3P protocol downloads the privacy policy from each site, scans it, and notifies users if the policy does not match their preferences. In some cases, unethical marketers can post a privacy policy that does not accurately reflect how data is treated (George 2010). The W3C; an international industry group whose members include Apple, Ericsson, and Microsoft created P3P and is supporting its development. It sets out to achieve the ability of machines to detect the privacy level of a web site or a third party intermediary, such as a network advertiser or an analytics company and as well as while sending data (Brian, 2002).

Ethical use of information refers to the proper use of information in the way the owner of the information is pleased with. Currently, use of information in some websites is unethical which makes information sharing online a very ethical issue. The use of information wrongly can cause a lot of confusion and information theft such as identity theft, financial theft and other crimes associated with information theft. P3P sets out to help users of the web decide what part of their personal data and information is to be released and shared with other people. It creates a sort of privacy enhancement for the user so that users are certain of how they are represented online. P3P provides both a standard, computer-readable format for privacy policies and a protocol that enables web browsers to read and process privacy policies automatically. P3P enables the display of symbols that prompt users to take important decisions whenever a privacy policy is encountered online.

Hackers may use specialized computer software tools to gain access to customer information on any website (Bakare and Yisah 2015). There have being many news about how companies sell private information of their customers to other companies such as advertisement companies and also use customer personal information in unwanted ways, these constituted some of the fundamental reasons for the development of P3P. The levels at which customer's information will be disseminated are informed in the privacy policies of P3P. The P3P tools help web user to compare between various privacy policies and help the user to choose the best policy that suites his/her needs. This paper presents the effects of development of Platform for Privacy Preference (P3P) on ethical issues. The rest of the paper is organized as follows: section 2 discusses deployment of P3P Privacy Policies on Web Site, section 3 focuses on t*he impact of p3p developments on ethical issue, l*imitations of p3p and its ethical effects *are discussed in section 4 and section 5 focuses on findings. Section 6 discusses* related *works; section 7 focuses on future* work while section 8 concludes the work.

2. P3P POLICY ISSUES S*PECIFICATION*

P3P policies identify the data recipients and make a variety of other disclosures such as information about dispute resolution and the address of a site's human-readable privacy policy. The policies use an XML encoding of the P3P vocabulary to identify the legal entity making the representation of privacy practices in a policy, enumerate the types of data or data elements collected, and explain how the data will be used. The policies also cover all relevant data elements and practices excluding legal issues regarding law enforcement demands for information. P3P declarations are positive, meaning that sites state what they do, rather than what they do not do. The P3P vocabulary is designed to be descriptive of a site's practices rather than simply an indicator of compliance with a particular law or code of conduct. To address this issue, user agents may be developed that can test whether a site's practices are compliant with a law or code. The practices of the site is represented by the P3P policies. Intermediaries such as telecommunication providers, Internet service providers, proxies and others may be privy to the exchange of data between a site and a user, but their practices may not be governed by the site's policies (msdn, 2014).

2.1 P3P Ethical Knowledge based User Agents

On the Internet, an intelligent agent (or simply an agent) is a program that gathers information or performs some other services without your immediate presence and on some regular schedule (whatis.com, 2014). An agent is completely specified by the agent function mapping percept sequences of ethical knowledge based to actions.

P3P Ethical Knowledge based User Agents can be built into Web browsers, browser plug-ins or proxy servers. They can also be implemented as Java applets or JavaScript; or built into electronic wallets, automatic form-fillers, or other user data management tools. The agents look for references to P3P policy ethical related issues at a well-known location, in P3P headers in HTTP responses, and in P3P link tags embedded in HTML content. These references indicate the location of a relevant P3P policy. User agents can fetch the policy from the indicated location, parse it, and display symbols, play sounds, or generate user prompts that reflect a site's P3P privacy practices. They can also compare P3P policies with privacy preferences set by the user and take appropriate actions. P3P can perform a sort of "gate keeper" function for data transfer mechanisms such as electronic wallets and automatic form fillers. A P3P user agent integrated into one of these mechanisms would retrieve P3P policies on ethical issues, compare them with user's preferences, and authorize the release of data only if it certifies two conditions, firstly, the policy is consistent with the user's preferences and secondly, the requested data transfer is consistent with the policy (msdn, 2014). If one of these conditions is not met, for instance if there is a bridge on certain ethical issues, the user might be informed of the discrepancy and given an opportunity to authorize the data to be released, so that the blame will not be on the site.

2.2 Deployment of P3P Privacy Policies on Web Site

There are three steps for deployment of Platform for Privacy Preferences (P3P) specification (Fig. 1). The first steps involves translating the Natural Language Privacy Policy into a Full P3P Privacy Policy using an XML schema that can be read by user agents such as Microsoft Internet Explorer 6, this schema is defined by the P3P Project which is part of W3C. Nowadays, tools available that can help create a full P3P privacy policy.

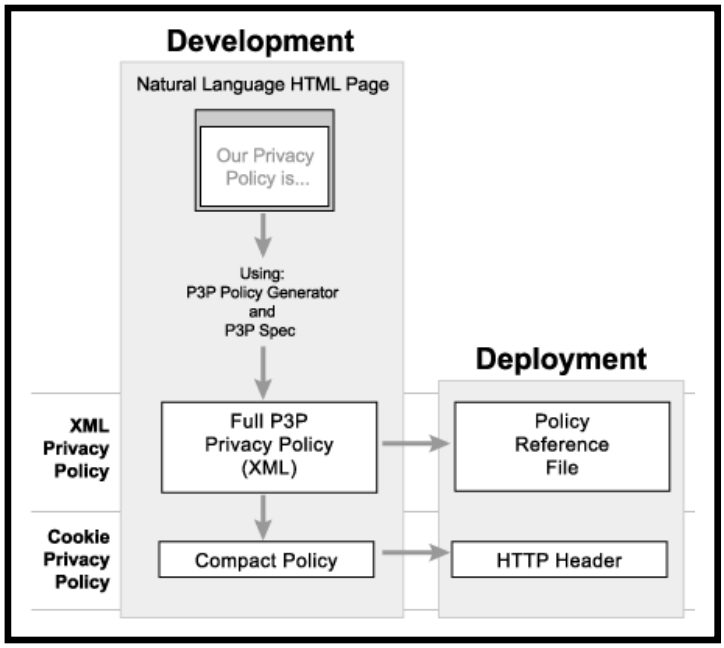

Fig1: Deployment of P3P Privacy Policies (**Source: msdn, 2014)**

In the second step, compact Policies for Cookies from the Full P3P Privacy Policy is created where all token representations of the full P3P privacy policy content are aggregated. These compact policies are used to indicate the privacy practices of a Web service that uses cookies.
In the third step, after the full P3P policies and compact polices are have being defined, they can be deployed on the Web site.

3. ETHICAL ISSUES

Ethics is a set of beliefs about right and wrong behaviour within a society. Ethical behaviour conforms to generally accepted norms, many of which are almost universal (George, 2000). According to Tene and Jules (2012), the principles of privacy and data protection must be balanced against additional societal values such as public health, national security and law enforcement, environmental protection, and economic efficiency. Moor (1989) defines the right to informational privacy as "the right to control of access to personal information." The definition contains four important elements. First, it is about *information*. This focuses on the quest for knowledge about someone, rather than, say, physical proximity or constraint, or any other type of interference. Second, it refers to *personal* information. The knowledge intended gives some access to the subject's person, whether it is his or her identity, thoughts, aspirations, passions, habits, foibles or transgressions. Third, the issue is one of *control*. It is not how much or how little is known about the subject, but whether the subject can choose how much of the information is revealed and to whom. Finally, privacy is defined as a *right*. Within certain "domains," as stated by Moor, the person's control of personal information ought to be respected and protected, but this is grossly violated on the internet.

3.1 Privacy Invasion

One of the major challenges facing internet users is privacy. Privacy has many meanings, according to Samuel D. and Louis D. (1960) in (The Right to Privacy, 2014), the most general, is freedom from interference or intrusion, the right "to be let alone,". This recognizes that each person has a sphere of existence and activity that properly belongs to that individual alone, where he or she should be free of constraint, coercion, and even uninvited observation, this sphere includes among other things, personal opinions and personal communications.

This broad concept of privacy has been given a more precise definition in the law, according to William Prosser (1960) cited in (www.stanfordlawreview.org, 2014), American common law has recognized four types of actions for which one can be sued in civil court for invasion of privacy.
These include:

i. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
ii. Public disclosure of embarrassing private facts about the plaintiff.
iii. Publicity which places the plaintiff in a false light in the public eye.
iv. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.

Without appropriate framework that define all the possible cases of privacy issues associated with internet users and implementation of the ideas into web browsers, invasion of user privacy will still remain.

3.2 The impact of P3P developments on ethical issue

Platform for Privacy Preference (P3P) enables machine-readable privacy policies that can be retrieved automatically by web browsers and by other user agent tools that can display symbols, prompt users, or take other appropriate actions. Ethical use of private information is a very important security issue because the information a user provides makes an image of the user. For example, name of a customer is vital information if it gets to wrong hands. If all pieces of information provided by the users is guaranteed to be secured on the internet, then users would at their will be given their information on websites without any fear of mismanagement. The current use of private information in unauthorized ways and the effects to the users of the internet is a major focus in this paper.
According to Robin, (2005), the concept of P3P arose from three main ideas:

i. A vocabulary for making and specifying privacy statements;
ii. A protocol for negotiating between the users and the website over privacy statements;
iii. A standard for storing personal information and controlling its transfer relative to 1 and 2.

P3P like most other internet standards was initiated in the United States in the early 90s. It was to focus on encouraging companies to post consumer readable privacy policies about their services. After discussions about this theory at the Internet Privacy Working Group, the idea of P3P was passed to the main standards setting body for the web that was charged with creating a P3P working group that would create the technical standards, the vocabulary, and the data schemas that would be used to make up the multiple choice questions and companies' standardizing their policies. Privacy policies are intended to describe a company's *data practices;* what they do with the information they collect from individuals (usually customers and potential customers, but sometimes also employees and others). This will bring clear progress in user privacy and information sharing. Part of the responsibility of the working group created by W3C is to fine tune the P3P idea, collect views from various levels of users and investigation of the legal aspect of the concept of the program.

The impact of Privacy for Platform Preference on Ethical issue is critical to the present stage of information technology. This is because the Internet is a center for sharing and storing information from every individual and organization all around the world. The way in which information from a particular individual meant for particular or specify number of users online is shared or stored without the consent of sender is unethical. P3P tries to check and develop how to create a standard on what type of user information should be revealed and how it should be revealed. It decides what format to use in alerting a user when his/her information is to be used. P3P seeks to use machine readable policies in achieving user's privacy while on the internet.

The developments of p3p has great positive impact on the ethical challenges face by internet users because now p3p is designed in such a way that it has standardized set of multiple-choice questions covering all the major aspects of a web site's privacy policies. These present a clear snapshot of how a site handles personal information about its users. The P3P specification considers ethical issues; it brings ease and regularity to web users wishing to decide whether and under what circumstances to disclose personal information. User confidence in online transactions increases as they are presented with meaningful information and choices about Web site privacy practices (Robin, 2005).

4. LIMITATIONS OF P3P AND ITS ETHICAL EFFECTS

The current limitation is the lack of a general framework to define all the possible cases of privacy issues associated with users and how to mobilize the ideas into web browsers. The collection of user data on the internet is not properly

standardized so it is difficult to create a policy on how these pieces of data will be used. Formulation of the standard for P3P by W3C which includes the syntax and semantics of privacy is also not a very familiar process; there is a need to improve on the efficiency in other to be useful worldwide.
The incorporation of P3P into websites by the designers also causes a hitch back for some website because the policy will reduce the amount of data they receive from their users.
On the part of browsers, incorporating P3P into the browsers requires lot of resources which at the time not affordable, for example the language specification, user's interaction with the P3P policies on the browser and many more.

5. Findings

Although P3P would make privacy policies transparent but it cannot ensure that companies follow privacy policies that have to do with ethical issues, because if a company says is going to do one thing and does something else, no technological process can stop it. Deception must be stopped through public policy processes, legislation and the courts (Michael, 2000). No technological process can ensure that companies comply with law or statements they choose to make. But, P3P will lead to greater openness, more informed web users and therefore greater accountability.

6. Related Work

Since Microsoft released their P3P-enabled IE6 web browser in 2001, an increasing number of web sites have adopted P3P. Survey carried out in December 2001 by the Progress and Freedom Foundation found that 23% of the most popular web sites and 5% of a random sample of the top 5,625 domains that collect personally identifiable data were P3P-enabled.
By April 2002, about a third of the top 100 web sites had adopted P3P (Jack, 2002). Early adopters of P3P from a variety of sectors include:

- Coremetrics, a leading web services provider of marketing analytics solutions
- News and information sites, such as CNET and About.com
- Search engines, such as Yahoo! and Lycos
- Advertising networks, such as DoubleClick and Avenue A
- Telecommunications companies, such as AT&T
- Financial institutions, such as Fidelity
- Computer hardware and software vendors, such as IBM, Dell, Microsoft, and McAfee
- Retail stores, such as Fortunoff and Ritz Camera
- Government agencies, such as the U.S. Federal Trade Commission, U.S. Department of Commerce, and U.S. Postal Service
- Nonprofit organizations, such as the Center for Democracy and Technology
- Academic institutions, such as Vanderbilt University eLab

Sites outside the U.S. have also started adopting P3P, such as commercial sites and the web sites of several data protection commissioners (for example, the Ontario Information and Privacy Commissioner and the Data Protection Commissioner of Bavaria, Germany). Many early adopters of P3P enabled their web sites to show their support for the P3P effort and demonstrate their corporate leadership on privacy issues. They were motivated both by a desire to show customers that they respect their privacy and by a desire to demonstrate to regulators that the industry is taking voluntary steps to address consumer privacy concerns. While P3P addresses only a narrow set of privacy issues, it complements other efforts to improve privacy protections, including laws, technology tools, and privacy seal programs.
Some companies have started using privacy as a way of distinguishing their brand; they include privacy messages in their advertising and feature privacy-related aspects of their products. By adopting P3P, they further strengthen the message that they respect consumer privacy. In addition, by adopting P3P, they enable consumers to quickly locate and get a brief summary of their privacy policies, and to take advantage of any opportunities to remove themselves from marketing and mailing lists. Some companies have adopted P3P in anticipation that it may soon become a standard that consumers look for at the web sites they visit. If consumers become accustomed to being able to request a privacy report from their web browser or to seeing a happy privacy-bird icon, they may grow suspicious of sites that are not P3P-enabled.

In the future, P3P-enabled search engines may make it easy for consumers to identify P3P-enabled web sites. Some companies have already found out that their web sites do not function correctly when viewed using the latest web browsers if their sites are not P3P-enabled. By default, IE6 looks for P3P compact policies associated with third-party cookies on web sites. Third-party cookies are automatically blocked when they don't have compact policies. Thus, targeted advertising, page counters, and other features that rely on third-party cookies may not work unless compacts P3P-enable their sites.
Finally, many web sites have adopted P3P because the individuals who run them value their personal privacy and want the companies they work for to take steps to give individuals more control over their personal information.

7. Future Works

Possible future work should include development of programs that will improve ethical usage of users' information.

8. CONCLUSION

In this paper, it was found that development of P3P has great impact on the ethical use of users' information. It was also found that proper standards for P3P would ensure proper use of users' information and vice versa. It was found that if P3P standards are properly created and proper awareness given, the public and the general web community will go for it. We found out that the reason why most people have not adopted P3P is that it is still not generally defined in all aspects of user's privacy. Implementation of P3P will lead to greater openness, more informed web users and therefore greater accountability.

REFERENCES

1. Bakare K. A. and Yisah S. O (2015). Employing the Concepts of Hacking as a Tool to Test Network Security and Data Protection. International Conference on Science, Technology, Education, Arts, Management and Social Sciences iSTEAMS Honours Conference, University of Ilorin, Nigeria. Proceeding Series 7, pp. 683-688.
2. Brian J. Z. (2002) Position Paper W3C Workshop on the Future of P3P
3. http://www.w3.org/2002/p3p-ws/pp/aol.html
4. George W. R. (2000). Ethics in Information Technology, Third Edition, Published by JoeSabatino, Course Technology, Cengage Learning pg.3
5. George W. R. (2010), Ethics in Information Technology, Course Technology, Cengage Learning. Pg 139
6. Jack H. (2002). P3P Position Paper: *Agents and P3P W3C Workshop on the Future* of P3P
7. Michael G., Deirdre M. and Art S. (2000). P3P and Privacy: *An update for the Privacy Community*, Center for Democracy and Technology pg 7
8. Moor J. H., (1989) "How to Invade and Protect Privacy with Computers," in Carol C. Gould (ed.), *The Information Web: Ethical and Social Implications of Computer Networking,* Boulder, CO: Westview Press (1989): 57-70.
9. msdn (2014) http://msdn.microsoft.com/en-us/library/ie/ms537341(v=vs.85).aspx
10. Robin C. (2005). The Platform for Privacy Preferences 1.1 (P3P1.1) Specification.
11. W3C Working Draft. 4-January-2005. *http://xml.coverpages.org/ni2005-01-20-a.html*
12. Tene O. and Polonetsky J. (2012) Privacy in the Age of Big Data: A Time for Big Decisions. Retrieved on 30th October 2014 from http://www.stanfordlawreview.org/online/privacy-paradox/big-data
13. The Right to Privacy (2014). Retrieved on 13th November 2014 from http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html in Samuel D. W. and Louis D. B., "The Right to Privacy," *Harvard Law Review*, 4 (5), (1890): 193-220, p. 195, citing Judge Cooley in *Cooley on Torts,* 2nd ed.
14. whatis.com (2014) Definition of Agent. Retrieved on 30th October 2014 from
15. http://whatis.techtarget.com/definition/agent-intelligent-agent
16. William L. Prosser, "Privacy," *California Law Review,* 48 (1960): 338-423. In www.stanfordlawreview.org/online/privacy-paradox/big-data Privacy in the Age of Big Data a Time for Big Decisions. Accessed on 13th November 2014.