

Personally identifiable information and ethics: use of cookies

[Business](#), [Industries](#)



Cookie Trails In today's era of technology, many people are concerned about internet privacy. Most concerns are usually sparked by misinformation. One piece of technology that is most misunderstood is the cookie and its uses. Many people believe that cookies are programs that can transfer viruses onto their computers. This is absolutely false. Cookies are typically harmless. Cookies are little text files left on your hard disk by some websites you visit (Williams & Stacy C. Sawyer, 2013, p. 05). These text files store information about the user like preferences, log-in name, and password. Cookies can be very beneficial for users who frequent many sites. It is very convenient to forgo having to remember every user name or password for every site you visit on a regular basis. Another convenience is using the shopping cart feature of a retail site. For instance, you have added items to your cart, and suddenly lose internet connection. Once internet connection is restored and you return to the site, your shopping cart items are still listed there.

Websites also benefit from using cookies. Sites can store user preferences with the purpose of having a unique appearance for each user. Sites can also use cookies to track how many visitors a site receives. This particular piece of information is vital for sites who offer free access. Lately, many consumers have been distressed over how websites are using tracking cookies. Tracking cookies could potentially amass a compilation of all your browsing habits. Marketing companies such as DoubleClick have taken tracking cookies a step further. The cookie it dispatches will come alive every time you visit another site that does business with DoubleClick" (Peneberg, 2005). DoubleClick can then take that information it has gathered and pair it with personally identifiable information like a phone number or email, and most troubling a

home address. DoubleClick was pummeled six years ago when it announced its intent to create a database of consumer profiles that would include names, addresses, and online purchase histories.

After public outcry and a class-action suit (which was settled in 2002), DoubleClick did an about-face and said it had made a huge mistake (Peneberg, 2005). When cookies are used in this manner it definitely brings ethical issues to the forefront. It is an invasion of privacy to take, use and potentially sell information that was not knowingly shared. It is an abuse of privileges users innocently extend to websites. If this invasion of privacy is allowed to continue, one could only wonder what will await the unsuspecting user in future.

It is quite plausible for large marketing and advertising firms to start tampering with cookies, eventually creating more evasive ways of snooping on users, and in the process obtaining more crucial information like social security numbers. Marketers don't fear that the government will ban or restrict cookies someday. After heavy lobbying they managed to secure an amendment to the Securely Protect Yourself Against Cyber Trespass Act that would exempt cookies from any spyware legislation that passes in the House (Peneberg, 2005).

The people could rally together to band cookies, but that would make browsing the web difficult for all. It would make more sense to establish stricter regulations against tracking cookies. When companies start to dig too deep and go too far, the people will rebel. Cookies should remain just

simple text files that mutually benefit the site and the user. There is no need to invade users' privacy for profit.

References

1. Peneberg, A. L. (2005, November 7). Cookie Monsters: The innocuous Text Files that Web Surfers love to hate.
 2. Retrieved November 5, 2012, from Slate: http://www.late.com/articles/technology/technology/2005/11/cookie_monsters.html
- Williams, B. K. , ; Stacy C. Sawyer. (2013).