International Baccalaureate

Extended essay cover

Candidates must complete this page and then give this cover and their final version of the extended essay to their supervisor.

Candidate session number			
Candidate name			
School number			
School name			
Examination session (May or November)	May	Year	2013

Diploma Programme subject in which this extended essay is registered: ITGS

(For an extended essay in the area of languages, state the language and whether it is group 1 or group 2.)

Title of the extended essay: What are the risks associated with the usage of cookies for intermediary web users in the context of social and ethical concerns?

Candidate's declaration

This declaration must be signed by the candidate; otherwise a grade may not be issued.

The extended essay I am submitting is my own work (apart from guidance allowed by the International Baccalaureate).

I have acknowledged each use of the words, graphics or ideas of another person, whether written, oral or visual.

I am aware that the word limit for all extended essays is 4000 words and that examiners are not required to read beyond this limit.

This is the final version of my extended essay.

Candidate's signature:

Date:

Supervisor's report and declaration

The supervisor must complete this report, sign the declaration and then give the final version of the extended essay, with this cover attached, to the Diploma Programme coordinator.

Name of supervisor (CAPITAL letters)

Please comment, as appropriate, on the candidate's performance, the context in which the candidate undertook the research for the extended essay, any difficulties encountered and how these were overcome (see page 13 of the extended essay guide). The concluding interview (viva voce) may provide useful information. These comments can help the examiner award a level for criterion K (holistic judgment). Do not comment on any adverse personal circumstances that may have affected the candidate. If the amount of time spent with the candidate was zero, you must explain this, in particular how it was then possible to authenticate the essay as the candidate's own work. You may attach an additional sheet if there is insufficient space here.

This declaration must be signed by the supervisor; otherwise a grade may not be issued.

I have read the final version of the extended essay that will be submitted to the examiner.

To the best of my knowledge, the extended essay is the authentic work of the candidate.

I spent 1 hours with the candidate discussing the progress of the extended essay.

Supervisor's signature: Date

Assessment form (for examiner use only)

	Achievement level				
Criteria	Examiner 1	maximum	Examiner 2	maximum	Examiner 3
A research question	2	2		2	
B introduction	2	2		2	
C investigation	3	4		4	
D knowledge and understanding	4	4		4	
E reasoned argument	4	4		4	
F analysis and evaluation	3	4		4	
G use of subject language	4	4		4	
H conclusion	2	2		2	
I formal presentation	3	4		4	
J abstract	2	2		2	
K holistic judgment	3	4		4	
Total out of 36	32				

Extended Essay:
ITGS

Research Question: What are the risks associated with the usage of cookies for intermediary web users in the context of social and ethical concerns?

Candidate Name:
Candidate Number:
Session: May 2013
Supervisor Name:

Word Count: 3955

Abstract:

My recent studies in ITGS and interest in internet privacy and anonymity led to my desire to explore the research question of "What are the risks associated with the usage of cookies for intermediary web users in the context of social and ethical concerns?" Cookies are becoming more and more dangerous in their collection of personal data. Because of this, the social and ethical concerns most examined were related to privacy and policies. The investigation first looked at risks, both in the early and later developments of the technology, followed by its benefits and possible solutions to amend the information crisis.

The essay looks at a mixture of articles and studies performed surrounding cookies. In the early risks, privacy concerns are investigated in the collection of personal data, inadequacy of security systems surrounding this data, third-party cookies, and the failure of cookie protocols. In the later risks, heightened privacy risks are examined in the collection of psychographic information, creation of audiences, effect of this information on real life, supercookies, digital fingerprinting, and the do not track standard. Benefits of targeted advertising are then examined, culminating to the conclusion that cookies must be kept for the survival of websites and the companies they represent. Solutions, based on the failed cookie protocols of the IETF and new policies created in the EU e-privacy directive are analyzed.

I concluded that the main problem behind cookies was their lack of proper standards and that the system must be repaired as companies, and the internet, depend on the technology. Following the e-privacy directive along with standardized IETF policies is the most logical solution to the problem.

Word Count: 271

Table of Contents:

Abstract........3

Introduction........4

Background........5

Early Risks........6

-Privacy and Security........6

-Standards and Protocols........8

New Risks........9

-Privacy Risks- Ad-Tracking and Ad-Servicing........9

-Privacy Risks- Exploitation........11

-Policy Risks........13

Benefits........16

Solutions........17

Conclusion........18

Bibliography........20

Introduction:

My research question is: what are the risks associated with the usage of cookies for intermediary web users in the context of social and ethical concerns? For clarification, an intermediary web user is someone who has little to no understanding of cookies[1] and therefore cannot protect his/her information adequately.

More and more people use the internet on a regular basis to tap into its enormous wealth of free knowledge and content. However, as I discovered in my ITGS classes, as increasing number of people use the services and reap the benefits of the internet, many do not understand that this "free" system comes with costs and risks. Many businesses are using cookies – small packets of code that track information about users – to gather a vast web of personal information. This amalgamation of information has made cookies a dangerous and surreptitious way of collecting personal data unbeknownst to the everyday web surfer.

Almost every person who has surfed the web has had a cookie implanted in their computer. An investigation of cookies is worthy of further analysis because of 1) the privacy and security concerns that have risen from the usage of cookies to collect data and 2) the sustainability of advertising revenue by website operators. These problems, along with new developments such as supercookies and digital fingerprinting, make the discussion of cookies more relevant today than ever before. This investigation will analyze social and ethical concerns, such as privacy and standards, relating to cookies throughout their history. An analysis of primary and secondary resources (interviews, studies, and papers written in the field) will show benefits and risks associated. Potential solutions that would benefit users while acknowledging issues facing website operators will then be presented.

[1] Kessler, Online behavior tracking and privacy: 7 worst case scenarios (Mashable, 2010)

Background:

The advent of the cookie emerged from Netscape, the premier internet browser company in the early 90's. In 1994 the internet was a growing phenomenon rife with problems. Especially troublesome was the development of Ecommerce, a business that Netscape was determined to help succeed[2]. To improve their system, Lou Montulli, an employee at the company, was tasked with addressing the inability for the internet to remember user-specific information and settings. He fixed this problem by making the cookie.

As stated by Tim Berners-Lee, creator of the internet, the internet was originally "stateless"[3], or that it had no memory. The biggest problem with this was that Ecommerce could never be much more than a vending machine, in that it could only sell products one at a time and never remember the products users showed interest in[4]. The purchasing process had to be continued from start to finish without the ability to visit other sites or look at other products. Montulli was able to fix the issue with cookies, text files acting as persistent client state objects that would "remember" user's actions[5].

In summary, the cookie provided the first persistent state information storage device which allowed websites to store name-value pair information on a workstation's hard disk[6]. However, the original cookies had limited uses. The first cookie was simply used to find whether users visited the Netscape homepage multiple times[7]. Later, cookies would be used for tasks such as remembering user preferences, passwords, and checkout IDs[8]. Now, cookies can be created

[2] Clark, Netscape time: The making of the billion-dollar start-up that took on microsoft (1999)
[3] Berners-Lee, Hypertext transfer protocol design issues (1991)
[4] Shah, The role of institutions in the design of communication technologies (2001)
[5] Schwartz, Giving the web a memory cost its users privacy (2001)
[6] Brain, How internet cookies work (n.d.)
[7] Vieux, The once and future kings (1995)
[8] Senatore, Cookies and your privacy: Past, present and future (2011)

many different ways and complete tasks ranging from remembering passwords to user surveillance.

Early Risks:

The early risks of cookies pertain to problems that were inherent or emerged very early in its development. Risks inherent in cookies were associated with the breaches in privacy caused by tracking, uncertain security measures of the information, and a lack of standards throughout its growth.

Privacy and Security:

What originally began as simple solution, cookie has now become dangerous for users of the internet. The gathering of data such as page views, visitor sessions, usernames, passwords, and personal settings in individual websites, when attached to a specific IP address, provides a "digital profile" for many websites that cannot be verified, fact-checked, or deleted by the public[9]. Information about user preferences on websites was not expressly given by users to companies, and therefore many believe it should not be tracked at all. This privacy concern also creates a security concern, as users do not want this data to be compromised. The collected data is usually stored in a database to easily record, store, and retrieve specific information pertinent to the website's needs. Though many websites refer to their encoding and encryption[10], along with security measures such as SSL (Secure Socket Layer), as measures to ease the public consciousness, the ability to decode and decrypt database information connected to individual users is surprisingly simple. Back in 1995, couple of UC Berkeley graduate students was able to crack the security code used by Netscape to protect internet credit card transactions. Moreover, Netflix inadvertently exposed private video preference records of its customers despite best

[9] Online Privacy Alliance, What is cookie profiling? (1998)

[10] Online Privacy Alliance, Privacy concerns on cookies (1998)

efforts to hide their identities[11]. These instances highlight the inadequacies of early security measures protecting personal information.

The privacy concerns posed by cookies were further augmented with the creation of third-party cookies. In 1996 Bell Laboratories, headed by computer scientists Koen Holtman and David Kristol, formed a team to help improve cookies[12]. What they discovered was that cookies on a site do not have to be the exclusive property of the site owner. Websites, instead, could agree to place cookies across a network of other sites. These cookies, unlike first-party cookies placed by the site itself, are known as third-party cookies, and present their own breed of privacy problems. If the network of sites is large enough, it can track users throughout all websites they visit. This means the breath and coverage of user data would increase. This eventually would pave the way to ad-tracking and ad-serving technologies built off of cookies. As early as 1996 startups were being formed, such as Engage, Infoseek, and Doubleclick, to collect user profiles and create ad networks for targeted advertising[13]. Eventually, Doubleclick became a leader of the new ad networking business, developing ad services along with a library of user profiles and related data such as contact info and personal interests[14]. These companies would use cross-site profiling to find matching preferences and sell this private information to advertising companies[15].

Cookies originally were a privacy hazard because of their ability to gather personal internet browsing information and compile it into databases whose content and level of security risk were of unknown quality. Third-party cookies then allowed private information to be

[11] Abate, Finding chinks in netscape's armor (1995)
[12] Schwartz, 2001
[13] Ads find strength in numbers (1996)
[14] Kornblum, Doubleclick launches ad service (1998)
[15] Brain, n.d.

amassed across many websites, categorized, and then sold to advertisers, making such private information a public commodity.

Standards and Protocols:

Though the privacy concerns of cookies were significant, they could not have become so deleterious for users without inappropriate and sometimes nonexistent standards for cookie implementation and usage. The Internet Task Force, an organization started by Bell Laboratories[16], began to create policies to stop data collection from companies like Doubleclick by ending the practice of counting unique user IDs[17]. It called for implementation of these rules across the web. The IETF wanted to prohibit major browsers from supporting all third-party cookies[18]. The inability to count unique users would stop the personalization of the data while elimination of third-party cookies would stop excessive web tracking. Attorney General of Michigan, Jennifer M. Granholm, at one point, said Doubleclick was a "secret cyber-wiretap"[19], because consumers are not aware that their online activities are being monitored and collected.

Third Party Tracker	Number of Sites
Doubleclick.net	73
Scorecardresearch.com	58
Adnxs.com	48
Quantserve.com	47
Ad.yieldmanager.com	42

Top 5 Third Party Trackers for Top 100 Sites

[16] Schwartz, 2001

[17] Coale, Doubleclick tries to force hand into cookie jar (1997)

[18] Kristol, Http state management mechanism (1997)

[19] Mayer, Doubleclick is probed on data collection (2000)

However, after these events, the standards were repealed, creating the root of the privacy dilemma. The IETF and its policies were eventually disregarded and discarded[20]. The Federal Trade Commission cleared Doubleclick, allowing it to pursue the same policies as before[21]. The Securely Protect Yourself Against Cyber Trespass Act of 2005, which would have protected internet users from having their information privately transmitted through spyware programs (like cookies), died in the senate[22]. Because of this, it is now standard for a browser to have no restrictions regarding third-party cookies. Without these proper standards, third-party cookies, data transfer, and tracking were all left untouched.

New Risks:

Starting in late 2008, with growing popularity of social networking sites like Facebook, there has been an increase in targeted advertising which required the reevaluation of the risks of cookies. Many of the new risks are built on the growing trend in escalation of the usage of cookies to collect information and advertise. This section will contain three parts, an explanation of the amalgamation of more data, the exploitation of this said data, and the lack of policies in this system.

Privacy Risks- Ad-Tracking and Ad-Servicing:

One of the largest and most well-known problems associated with cookies today is their excessive tracking, or propensity to collect more data than a user would even fathom. In the past, cookies were mainly used to find patterns in purchasing or behavior to discover your preferences. Joanna O'Connell, a researcher for the marketing research firm Forrester Research, who follows online advertising, says that the old data gathered is only a fraction of what is

[20] Kristol, 1997

[21] Associated Press, Ftc clears doubleclick (2001)

[22] Congressional Research Service, Securely protect yourself against cyber trespass act (2006)

collected now, as new data collected include "gender, age, income, and number of children". Non explicit Psychographic information as in whether the person is introverted or extroverted, and political leanings, as in liberal or conservative, are being collected.[23] The popularity of smartphones also pose problems as new mobile ad technologies have the ability to tap into a wider amount of personal data. As Chris Conley of the ACLU states, smartphone cookies have "access to your contacts, geo-location, call records, and other information that's stored on your phone". Applications like Path, a mobile social-networking app, upload names, emails and numbers of contacts in its users' phones without permission.[24]

The other trend is with the changing ad-servicing business, or the way information is presented and sold. During the early days of the Web, advertisers were fine with placing blind ads, or ads in front of people they knew little about, so that a few people from hundreds would click on them[25]. However, now that 84% of website's cookies and ads are managed by third-parties[26], advertisers have the power to follow a user's consumption patterns to predict future purchases. This has created a system of predictive analysis, where, according to the Wall Street Journal, advertisers are moving away from random "clicks" to "audiences", or people who have similar tastes in ads, products, and purchasing[27]. The problem with this model is it creates even more avenues for the intrusion of user privacy. A person, who may be shopping for Christmas products at one site, will now be followed by ads displaying gifts at other sites he visits. Like the infamous incident where Target, based on vast amounts of data collected from their customers, was able to create a list of women likely to be pregnant. These women were sent specific coupons for baby clothes and cribs, and one of its targets turned out to be a young girl still in

[23] Sydell, Smart cookies put targeted online ads on the rise (2010)
[24] Karas, 10 things online data collectors won't say (2012)
[25] Sullivan, Data snatchers! the booming market for your online identity (2012)
[26] Hoofnagle, Web privacy census (2012)
[27] Stecklow, On the web, children face intensive tracking (2010)

high school.[28] When her dad discovered these coupons, it obviously meant that their personal lives were out in the open to Target's analytics department. Companies routinely collect all products purchased by individuals as well as buy demographic information from third parties therefore causing the privacy problem to expand.

Privacy Risks- Exploitation:

The personal information gathered presents another problem as it affects the way people are being presented in real life. Using the internet information, companies and institutions are making decisions such as whether you get a credit card, job, or which political party you get messages from.

The phenomenal growth of social networking sites such as Facebook, Google+ and Twitter naturally collects and stores information that's been voluntarily supplied by millions of its members with varying degrees of privacy protection. Recently, private companies and even college admission officers have used the Facebook application or simply the profile photos that appear on site as a tool when evaluating a job candidate or college applicant. Studies have shown, more than one-third of people's application forms are judged against what they post or the persona on the web[29]. This new risk has forced many students to try to purge or scrub their profiles of incriminating material or change their names to avoid detection[30].

If people are afraid of private information they provide willingly to social networking sites becoming exposed unwittingly to HR departments or college admins, the massive wealth of unknown and more personal information held in cookies would be even more shocking. Jeff Chester of the Center for Digital Democracy, says as people continue to handle more of their

[28] Duhigg, How companies learn your secrets (2012)

[29] Hunt, Thirty-seven percent of companies use social networks to research potential job candidates, according to new careerbuilder survey (2012)

[30] Maslin, An online alias keeps colleges off their trail (2010)

personal business online, from health matters to personal finance, advertisers could begin gathering information that many would not want to share[31]. There is a dangerous line when personal data becomes the basis of an individual getting health insurance or qualifying for a job[32]. Already, public records sites such as Intelius, Spokeo, and PeopleFinders.com distribute the kind of data that landlords, insurers, employers, or creditors could easily use to screen applicants[33]. This information is available to everyone for only a nominal fee. The bottom line is that cookies used to gather information that would only affect the ads you see on the internet, but now are a larger privacy threat in their ability to affect your life.

Policy Risks:

The lack of policies surrounding cookies creates problems with an individual's digital rights because of the double-standards and deceitfulness in the tools used to delete cookies, including the "do not track" standard.

The first problem surrounding policies is that user's efforts to delete cookies are not respected by companies that benefit from distribution of cookies. Newer technologies have been developed to make cookies better and more difficult to delete. Currently, there are no policies regarding the removing of cookies, and companies are free to counteract efforts to eliminate cookies. There has been a constant improvement in anti-virus software industry to actively remove malware and cookies, but cookie creators have worked just as hard to stay a step ahead and avoid being completely removed from systems or cookie erosion. In 2011, researchers at Stanford University led by Professor Jonathan Mayer, found supercookies, cookies that recreate user's cookies after the user deletes them[34]. Supercookies are a direct outcome of the lack of

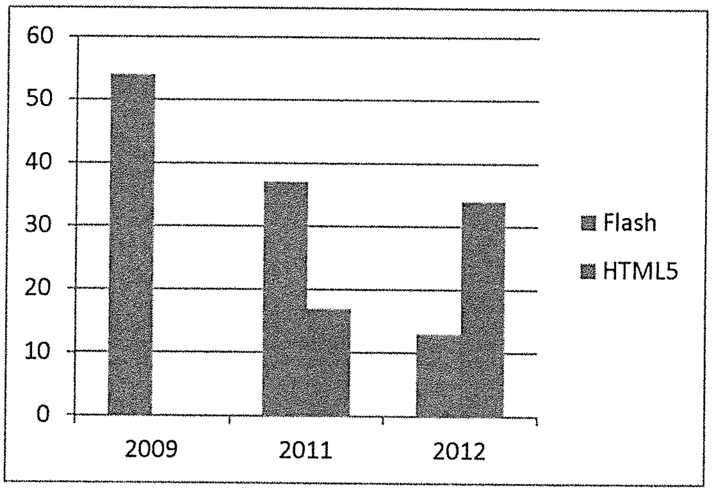
[31] Sydell, 2010

[32] Karas, 2012

[33] Sullivan, 2012

[34] Fischer, Microsoft drops use of 'supercookies' on msn (2011)

cookie policies. With improvement in spyware removal programs, the amount of Flash cookies, an early version of supercookies, dropped dramatically, to about 25% of its original levels on the top 100 websites according to the Web Privacy Census studies in 2011[35]. However, according to Chris Hoofnagle, director of the information privacy programs at the Berkeley Center for Law & Technology, the usage of HTML5 cookies doubled while Flash cookies declined. Hoofnagle says that HTML5 cookies, because of their status as a technology made for a developing standard, could be even more difficult to block[36]. Companies easily create new technologies to replace or perform similar actions to those denounced before. Without a permanent policy, there is no guarantee of an effective or complete protection.



Intrusive technologies are also reducing user's right to anonymity on the internet. Digital Fingerprinting can match a person to their digital profile regardless of the computer used or how many times cookies are deleted. In the past, two main challenges to using cookies were cookie erosion from improving spyware or anti-virus applications and the difficulty in tracking multiple users on a single workstation. BlueCava addressed this multiple user issue with its "device ID" technology that finds unique website settings and preferences to identify a specific user and match him/her with their correct profile[37]. BlueCava CEO David Norris says that his company's technology can identify devices with 99.7 percent accuracy. This ability to match users, says Kaliya Hamlin of the Personal Data Ecosystem Consortium, will degrades privacy by taking

[35] Temple, Web privacy census shows tracking pervasive (2012)
[36] Temple, 2012
[37] Sullivan, 2012

away our ability to use alternate identities online to keep certain aspects of our digital lives separate. Michael Fertik, chief executive of Reputation.com, a service that works to keep its customers information private, says that 10% of the records it removes via removal requests and anti-cookie software reappear the next day, meaning the information is never really deleted, just stored for later usage[38].

Finally, the most confusing standard according to many is the "do not track", or "opt out" standard, which is applied differently for every company. Studies have shown that web users believe "do not track" will stop the collection of personal data, but in reality the only thing it stops is targeted advertising. The Digital Advertising Alliance of 2010, despite providing users web alerts that their data was being collected and tracked to feed targeted advertising, and provided an opt out plan, information was still collected after the implementation of the opt out[39]. Linda Woolley, executive vice president of the Direct Marketing Association, says every click was still recorded and stored. Do Not Track, which many people rely on for anonymity, is not a standard set in stone, so companies use the false promise of safety to steal more info.

The lack of defined policies enables companies to freely use cookies to actively violate digital rights from web-users. Anonymity, the most basic allure of the internet, may be threatened by these practices.

Benefits:

So why wouldn't the solution be to simply ban cookies permanently? Because, even though cookies create a whole host of problems, they are also needed for the internet as we know it to function. Cookies' status as a "virtual license plates" allows them to perform meaningless and tedious tasks such as remembering "login and password, the products you've just bought, or

[38] Angwin, Sites are accused of privacy failings (2012)
[39] Karas, 2012

your preferred color scheme"[40]. However, the benefits of cookies go beyond their intended use. Cookies are needed for the survival of the companies they benefit.

Cookies are needed because they allow websites to produce the amount of ad revenue they need to function. Ad buyers, who have to navigate through and decide on thousands of websites and millions of pages, need information from the websites about the type of users the advertisers are selling to. This is the reason why, as Su Doyle, marketing director for AdSmart.net, states, marketers need audiences so that they can easily target their niche groups[41]. To collect and build audiences require third-party networks and third-party cookies, with the quality of information depending on the amount of data and the size of the network. Moreover, The Network Advertising Initiative released a study that found behaviorally targeted advertising secured more than 2.5 times as much revenue per ad as its non-targeted counterpart[42]. Fewer targeted ads could mean less revenue for both advertisers and websites, forcing websites to institute paywalls – a system to prevent people from accessing web content for free – for monetization. If cookies ever become illegal, websites may not be able to provide the amount of free content it does today. Many people, including Christopher Soghoian, a privacy advocate who studies data security and privacy at Indiana University, say that "the web was free for the last 15 years before they were tracking people, and it will continue to be free after they track people"[43]. But, before tracking the web was much smaller than it is now. Now, industries such as newspapers and magazines completely depend on revenues from their website ads[44]. A solution cannot be to permanently ban or restrict cookie usage to minimize data collection.

Solutions:

[40] Penenberg, Cookie monsters (2005)

[41] Ads find strength, 1996

[42] Kessler, 2010

[43] Kessler, 2010

[44] Levy, The changing business of journalism and its implications for democracy (2010)

The collection of personal data would not be a problem if there was stricter restriction from the types of exploitation that is rampant today. An ideal solution could be to increase user awareness of cookies combined with strong standardized rules surrounding the implementation and scope of personal data collection, without stifling the marketing and advertisement sector. One possible solution, adopted in Europe, is based on the new E-Privacy directive.

- IETF standards: As stated previously, standards made by the IETF and other agencies that were struck down in the past could be utilized for the same merits they posed before.
- Educating the Public: One of the main reasons why the public cannot mount a considerable offense against cookies is due to their lack in awareness. In an August 2010 study about Internet users' understanding of behavioral advertising, only 51% of participants recognized what targeted advertising was, and only 30% believed personal information would be used[45]. The IAB has created educational videos on the benefits of behavioral advertising to stop public misconceptions on the usage of cookies for the EU[46]. With a more informed public, lawmakers and companies may be pressured to amend the cookie policy.
- Opt-In: Opt-in is a system where users have to accept website's cookie policies before accessing the site[47]. Though many call it an "unworkable" and "inappropriate" standard[48], users must give "explicit consent" to accept cookies for accessing their desired sites, meaning sites still have leverage to gain viewers, while being completely open about data collection.

Conclusion:

[45] Kessler, 2010

[46] IAB, Your online choices (2011)

[47] Arthur, Eu e-privacy directive takes effect may 26 --will your cookies crumble? (2012)

[48] Kessler, 2010

Cookies are a primary conduit for collection and hosting vast amounts of personal data without consumer knowledge or protection, but the ability to repackage that data for commercial purposes must come with tighter rules and regulations. In order to circumvent cookie erosion applications that are available in the market, cookie makers have developed even stronger versions to collect even more data and better target users. Consequences have ranged from privacy intrusion to exposure of personal data that could negatively impact real lives while making billions of dollars to collectors of personal data from usage of cookies. Despite the best spyware or anti-virus applications or public awareness, the main reason behind continued usage of cookies is the surprising lack of standards, policies and regulations.

Reinitiating the standards that were discarded a decade ago, including those of the IETF, along with the main components of the E-privacy directive, increased public awareness and aggressive usage of opt-in, could force websites to be more accountable for their tracking and reduce information they gather to reasonable levels.

Bibliography:

Abate, T. (1995, Sep 20). Finding chinks in netscape's armor. SF Gate, Retrieved from http://www.sfgate.com/business/article/Finding-chinks-in-Netscape-s-armor-3307173.php

Ads find strength in numbers. (1996, Nov 4). Cnet, Retrieved from http://news.cnet.com/Ads-find-strength-in-numbers/2009-1001_3-243757.html

Angwin, J. (2012, Feb 13). Sites are accused of privacy failings. The Wall Street Journal, Retrieved from http://online.wsj.com/article/SB10001424052970204136404577207183258570186.html

Arthur, L. (2012, May 22). Eu e-privacy directive takes effect may 26 --will your cookies crumble?. Forbes, Retrieved from http://www.forbes.com/sites/lisaarthur/2012/05/22/eu-e-privacy-directive-takes-effect-may-26-will-your-cookies-crumble/

Associated Press. (2001, Jan 23). Ftc clears doubleclick. USA Today. Retrieved from http://usatoday30.usatoday.com/tech/news/2001-01-23-doubleclick.htm

Berners-Lee, T. (1991). Hypertext transfer protocol design issues. Retrieved from http://www.w3.org/Protocols/DesignIssues.html

Brain, M. (n.d.). How internet cookies work. HowStuffWorks, Retrieved from http://computer.howstuffworks.com/cookie1.htm

Clark, J. (1999). Netscape time: The making of the billion-dollar start-up that took on microsoft. (pp. 109-157). New York, NY: St. Martin's Press.

Coale, K. (1997, Mar 17). Doubleclick tries to force hand into cookie jar. Wired, Retrieved from http://www.wired.com/science/discoveries/news/1997/03/2615

Congressional Research Service. (2006). H.r. 29 (109th): Securely protect yourself against cyber trespass act (H.R. 29). Retrieved from GovTrack website: http://www.govtrack.us/congress/bills/109/hr29/text

Cullen, D. (2000, Jun 14). Another day, another doubleclick privacy pr disaster. The A Register, Retrieved from http://www.theregister.co.uk/2000/06/14/another_day_another_doubleclick_privacy/

Duhigg, C. (2012, Feb 16). How companies learn your secrets. Forbes, Retrieved from http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all

Fischer, D. (2011, Aug 19). Microsoft drops use of 'supercookies' on msn. Threat Post, Retrieved from https://threatpost.com/en_us/blogs/microsoft-drops-use-supercookies-msn-081911

Hoofnagle, C. (2012). Web privacy census. Unpublished raw data, Berkeley Center for Law and Technology, University of California: Berkeley, Oakland, CA, .

Hunt , R. (2012, Apr 18). Thirty-seven percent of companies use social networks to research potential job candidates, according to new careerbuilder survey. PR Newswire, Retrieved from http://www.prnewswire.com/news-releases/thirty-seven-percent-of-companies-use-social-networks-to-research-potential-job-candidates-according-to-new-careerbuilder-survey-147885445.html

IAB. (2011). Your online choices. Retrieved from http://www.youronlinechoices.com/uk/about-behavioural-advertising

Karas, T. (2012, Apr 5). 10 things online data collectors won't say. Smart Money, Retrieved from http://www.smartmoney.com/spend/technology/10-things-online-data-collectors-wont-say-1333598586287/?link=SM_hp_ls4e

Kessler, S. (2010, Nov 3). Online behavior tracking and privacy: 7 worst case scenarios. Mashable, Retrieved from http://mashable.com/2010/11/03/behavior-tracking-privacy/

Kornblum, J. (1998, Oct 5). Doubleclick launches ad service. Cnet, Retrieved from http://news.cnet.com/DoubleClick-launches-ad-service/2100-1023_3-216287.html

Kristol, D. (1997). Http state management mechanism. Informally published manuscript, Bell Laboratories, , Available from Standards Track. (RFC 2109)Retrieved from http://tools.ietf.org/html/rfc2109

Levy, D. (2010). The changing business of journalism and its implications for democracy. (1st ed.). Oxford: Peter Lang.

Maslin, S. (2010, Apr 23). An online alias keeps colleges off their trail. New York Times, ST8. Retrieved from http://www.nytimes.com/2010/04/25/fashion/25Noticed.html?adxnnl=1&ref=style&adxnnlx=1355285707-Ks1Vv4hZCNegz9LMNRtCDg

Mayer, C. (2000, Feb 17). Doubleclick is probed on data collection. The Washington Post, Retrieved from http://pqasb.pqarchiver.com/washingtonpost/access/49792657.html?dids=49792657:49792657&FMT=ABS&FMTS=ABS:FT&date=FEB 17, 2000&author=Caroline E. Mayer&pub=The Washington Post&desc=DoubleClick Is Probed On Data Collection&pqatl=google

Online Privacy Alliance. (1998). Privacy concerns on cookies. Retrieved from http://www.allaboutcookies.org/privacy-concerns/

Online Privacy Alliance. (1998). What is cookie profiling?. Retrieved from http://www.allaboutcookies.org/cookies/cookie-profiling.html

Penenberg, A. (2005, Nov 7). Cookie monsters. Slate, Retrieved from http://www.slate.com/articles/technology/technology/2005/11/cookie_monsters.html

Schwartz, J. (2001, Sept 4). Giving the web a memory cost its users privacy. New York Times, Retrieved from http://www.nytimes.com/2001/09/04/technology/04COOK.html?pagewanted=1

Senatore, M. (2011, Apr 25). Cookies and your privacy: Past, present and future. Infosec, Retrieved from http://www.infosecisland.com/blogview/13304-Cookies-and-Your-Privacy-Past-Present-and-Future.html

Shah, R. (2001). The role of institutions in the design of communication technologies. Informally published manuscript, , Available from Arxiv. (TPRC-2001-086)Retrieved from http://arxiv.org/ftp/cs/papers/0109/0109109.pdf

Stecklow, S. (2010, Sep 17). On the web, children face intensive tracking. The Wall Street Journal, Retrieved from http://online.wsj.com/article/SB10001424052748703904304575497903523187146.html

Sullivan, M. (2012, Jun 26). Data snatchers! the booming market for your online identity. PCworld, Retrieved from http://www.pcworld.com/article/258034/data_snatchers_the_booming_market_for_your_online_identity.html?page=2

Sydell, L. (2010, Oct 5). Smart cookies put targeted online ads on the rise. NPR. Retrieved from http://www.npr.org/templates/story/story.php?storyId=130349989

Temple, J. (2012, June 6). Web privacy census shows tracking pervasive. SF Gate, Retrieved from http://www.sfgate.com/technology/dotcommentary/article/Web-Privacy-Census-shows-tracking-pervasive-3663642.php

Vieux, A. (1995, Nov 1). The once and future kings. Red Herring Online.