Bittersweet cookies.
Some security and privacy considerations

Abstract

Cookies have emerged as one of the most convenient solutions to keep track of browser – server interaction. Nevertheless, they continue to raise both security and privacy concerns due to their continuous evolution, which addresses the needs of industries (i.e. advertising companies). In this paper, we identify and briefly analyse some of the most common types of cookies in terms of security vulnerabilities and the relevant privacy concerns. There is limited support for confidentiality, integrity and authentication in the way cookies are used. In this respect, the possibilities for misusing cookies are very real and are being exploited. Furthermore, due to the nature of the information they store and the way cookies are used for profiling, privacy concerns have been raised and policy initiatives have been initiated to address such issues. This paper takes into consideration the new types of cookies now being deployed in the online environment; these new cookies do not have enough exposure to demonstrate how they are being used and, as such, their security and privacy implications are not easily quantifiable. Studies are required to identify to what extent the new cookies can be used for tracking and also to evaluate the level of identification provided. Regarding policy perspective, the relevant EU legal framework that also addresses cookies is in transition. Currently, Member States are in the process of transposing EU directives addressing cookies and there is space for interpretations and clarifications. A study is required at the end of the transposition process to evaluate possible different requirements or interpretations.

Rodica Tirtea*, Claude Castelluccia+, Demosthenes Ikonomou*

* ENISA – European Network and Information Security Agency
http://www.enisa.europa.eu/

+ INRIA – Institut National de Recherché en Informatique et Automatique
http://www.inria.fr/

1. Introduction

Cookies have been designed to facilitate a browser-server stateful interaction, in a stateless protocol.

They are widely used by online service providers. Based on the results of a survey [1] carried out during 2010 by ENISA[1], almost 80% of online service providers interviewed are collecting data from cookies.

Internet Engineering Task Force (IETF) initiated in 1995 a standardisation process for cookies[2] [3]. In 2000, IETF published the RFC 2965[3] "HTTP State Management Mechanism" [4], which specify a way to create a stateful session with HTTP requests and responses.

Even during the standardisation process, privacy concerns have been raised, especially for third-party cookies [3]. As result of these concerns, cookies and their privacy implications have received media attention.

Meanwhile, new techniques have been deployed and new capabilities have been added to address requirements of the market and, as a result, *new types of cookies* are available today, with improved tracking capabilities, i.e. supercookies, Flash cookies [5, 6].

In this paper, we identify and briefly analyse some of the most common types of cookies in terms of security vulnerabilities and privacy concerns. The purpose of this paper is to highlight some of the security and privacy concerns generated by the use of cookies, without exhaustively identifying all of them; it is intended to serve as a starting point for further analysis by different communities.

A presentation of how cookies function and why they are used is provided in the following section. Sections 3 and 4 address security vulnerabilities and privacy concerns related to cookies. Policy perspectives are also included in section 5. Section 6 summarises the paper and provides some recommendations.

2. About cookies

Customised layout, capture of language preferences on a web page, identification for shopping list purposes at online shops, etc. are examples of our everyday life interaction with cookies. Servers adjust their response to each query with the information stored in the cookies from previous interactions.

Cookies, also known as *HTTP* (Hypertext Transfer Protocol) *cookies*, are generated and modified by the server, stored by the browser and transmitted between browser and server at each interaction.

The HTTP communication protocol is designed with the aim of allowing scaling through stateless operation. Using only such a protocol, it is not possible for the server to correlate one request from a client with previous requests by the same client. However, in case of online transactions, where more steps must be followed and the server must be aware of previous actions, state management is required. Cookies are a common solution for this requirement.

1 In 2010 ENISA launched a new area of work on "Trust and Privacy in the Future Internet" (ENISA Work programme 2010 is available at: http://www.enisa.europa.eu/about-enisa/activities/programmes-reports). In relation to this, ENISA has been running a study covering online service models and their support for security, privacy and accountability [1]. Another perspective, from architectural side is presented in [2].

2 An early description of cookies was published by Netscape Communications Corporation on their website [3].

3 The RFC (Request for Comments) 2109, "HTTP State Management", was published in 1997, but due to certain limitations (e.g. incompatibilities), it was not followed by industry. RFC 2965 describes three new headers, Cookie, Cookie2, and Set-Cookie2, which carry state information between participating origin servers and user browsers [4].

2.1. How cookies work

In Figure 1 we illustrate how cookies work; the main steps of the process are presented to facilitate the understanding of terminology used in this document.

Step 1. The client contacts the web server for the first time; in response to this request for web page content, the server generates a *session identifier (id)*, which will be part of a *cookie*.

Step 2. The server sends the *cookie* to the client, as part of the headers of the web page; the cookie is then stored by the client's browser. Note that this cookie will be communicated to the server each time the client issues a new query to the server. More specifically, each time a user enters a URL (Uniform Resource Locator) in a browser, the browser searchers its local memory to establish whether it has any cookie associated with it. If a cookie is found, it is inserted in the query sent to the server.

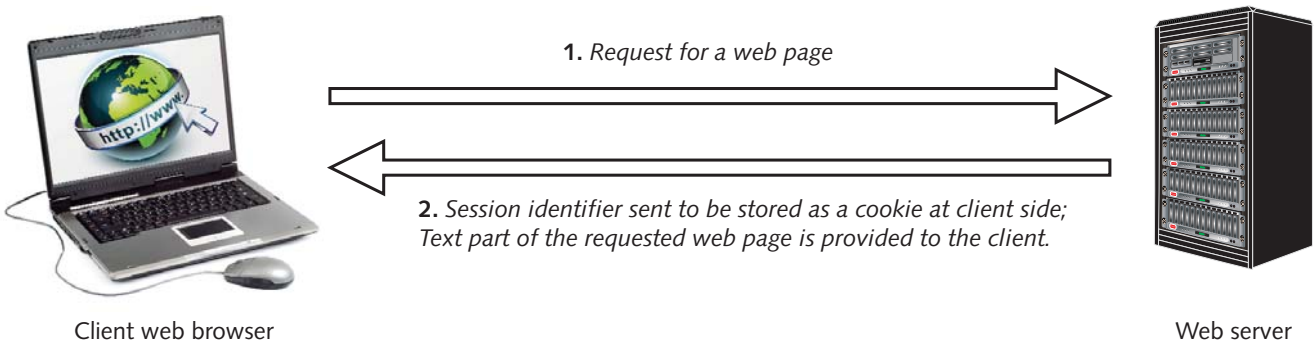

Figure 1: Illustration of cookies operation

Step 3. The web page content is gradually retrieved from the web server(s). The text part of the content is received first; note that a web page may contain some links, identified by URLs, to additional contents, such as images, animations, video or advertising that are fetched gradually. These URLs could point to the original web server (from where the text has been received, also called the *first party* server), or to other web servers (*third party* servers). In other words, a single web page can incorporate content from more than one server.

First party cookies are associated with the web server indicated by the URL of the page the client is visiting; they are set by the first party server (please refer to Figures 1 and 2). RFC 2965 [4] describes three headers, Cookie, Cookie2, and Set-Cookie2, which carry state information between participating origin servers and user agents. For instance, the Set-Cookie2 response header comprises the token Set Cookie2, followed by a comma-separated list of one or more cookies. Each cookie begins with a NAME=VALUE pair, followed by zero or more semi-colon-separated attribute-value pairs. Attributes are of types 'comment', 'domain', 'max-age', and 'secure'. Information for the user is stored in 'comment' attribute; 'max-age' stores the lifetime of the cookie. 'Secure' attribute specified in RFC2965 is optional. If the 'secure' attribute is set, then the cookie will be sent only over a secure communication channel.

Third-party cookies are extensively used by advertising companies. These cookies can be received by the browser while the user is visiting a web page that contains third-party content (e.g. ads, images) from third-party providers (the illustration in figure 2 identifies third party servers).

In the case of advertising (and in general of third party content), space is reserved on the web page for content coming from a third party server. The client web browser sends queries, using the URL for remote content, to all third party servers requesting the content without notifying the client or asking consent. The user is not necessarily aware of which third party servers are contacted and which information is provided to them.

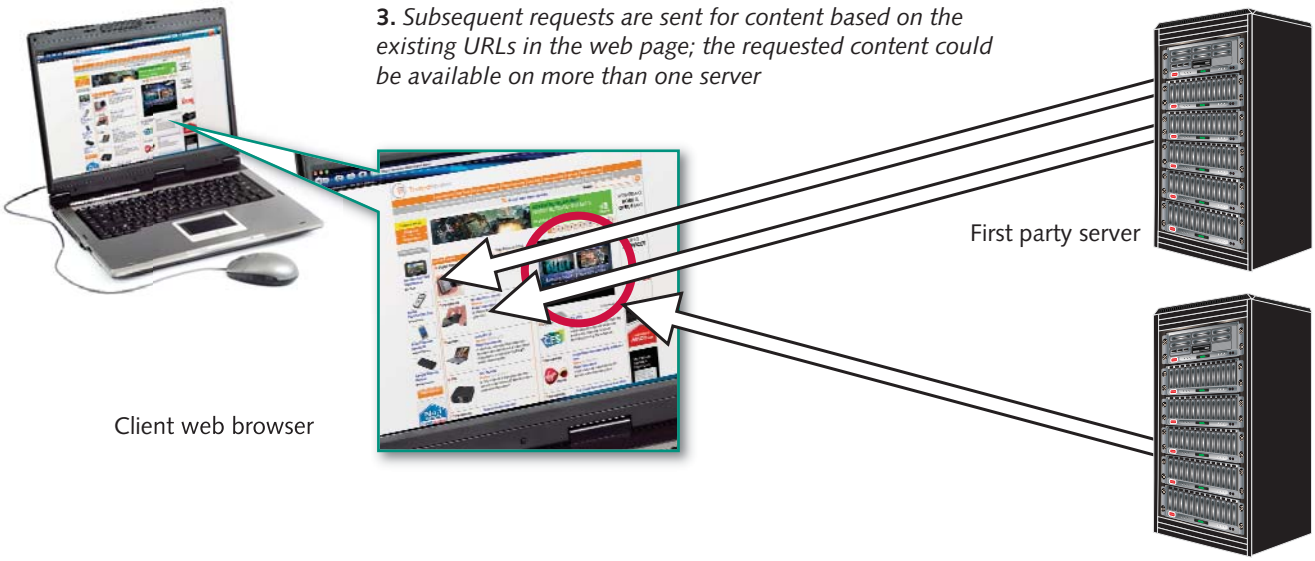

Figure 2: Third party content and cookies

Since online advertising companies need to accurately count the number of unique users and profile users, new and more persistent types of cookies[4] have emerged: ***supercookies, Flash cookies, evercookies, ubercookies*** **[5, 6]**. They usually rely on mechanisms able to track users outside the control of the browser. *Local shared object (.lso)* files, also known as *Flash cookies*, are used to store, in a more persistent manner, users identifiers **[5]**. They are also sometimes used to recover deleted cookies. Another example of super cookies is the Microsoft Internet Explorer userData **[8]**.

By default, all the activities related to storing and sending cookies are invisible to the user. Cookies can store a wide range of information (i.e. all the information previously provided by the user to a certain website), including personally identifiable information (such as user name, home address, e-mail address, or telephone number), which have been previously revealed by the user to online service providers.

Besides attributes (name, domain, expiration date, etc.), which are parts of the cookies, the following types of data can be stored in cookies:

- Credentials, such as user names and passwords and other identifiers
- Preferences and interface customisations/personalisation
- Session data and data from the site i.e. cached data
- Tracking information about users

Advantages of using cookies:

- From a functional perspective[5], cookies can be used for:
  - User identification and authentication (i.e. avoiding re-identification)
  - Statistics on number of visits, etc.
  - Storing preferences and settings

4 Scientific literature is scarce on this topic, however references to these powerful cookies can be found at [5, 6], and other web pages: Cookies, Supercookies and Ubercookies: Stealing the Identity of Web Visitors, 2010, available at: http://33bits.org/2010/02/18/cookies-supercookies-and-ubercookies-stealing-the-identity-of-web-visitors/ , Persistent Tracking using Supercookies and Evercookies, 2010, available at: http://www.securitygeneration.com/privacy/persistent-tracking-using-supercookies-and-evercookies/ , or Hacker Releases Tool for Producing the Ultimate Persistent Cookies, 2010, available at: http://news.softpedia.com/news/Hacker-Releases-Tool-for-Producing-the-Ultimate-Persistent-Cookies-157562.shtml

5 Animated explanations of advantages of using cookies: How can cookies make your surfing experience convenient? available at: http://www.animatedexplanations.com/Animation.aspx?animation=481 and http://www.iabeurope.eu/cookies-faq.aspx

- From a marketing and online advertising perspective, they could be used to:
  - Quantify/evaluate the efficiency of ads (i.e. making it possible to determine how many unique[6] users visited a site as a direct response to an ad)
  - Profile users and use the profiles to provide targeted advertising (i.e. behavioural targeting)
  - Improve management of advertisements (adaptation to user profile, rotation and duplication avoidance[7])

Compared with regular cookies, the new types of cookies have higher storage capacities. They are stored outside the browsers and are therefore more difficult to erase. Furthermore, they sometimes contain enough information to regenerate deleted cookies.

Implementation aspects. There are implementation limits on the number and size of cookies that a browser can store. According to RFC2965 [4], browser support should not have any fixed limits; however the following minimum capabilities are specified: at least 300 cookies; at least 4096 bytes per cookie (as measured by the characters that comprise the cookie according to the standard); at least 20 cookies per unique host or domain name. Browsers created for specific purposes, or for limited-capacity devices, should provide at least 20 cookies of 4096 bytes, to ensure that the user can interact with during a session with a server. On the other hand, applications should use as few cookies of as small a size as possible, and they should cope gracefully with the loss of a cookie [4].

Browsers may choose to set an upper limit on the number of cookies to be stored from a given host or domain name or on the size of the cookie information. Otherwise a malicious server could attempt to flood a user agent with many or large cookies, leading to a denial of service attack [4].

Compared to regular cookies, which fulfil the RFC2965 standard, supercookies such as userData [8], can hold up to 512KB per web page and 10MB per domain. Data can be written to the browser cache as an XML document and the data persists through re-boots and temporary folder deletions.

Some means to visualise and control storage for new cookies does exist. For instance, for Adobe Flash Player [9], storage settings can be specified using a panel that lists all the websites that the user is/ has visited. The following information is displayed in the list: the name of the website, the amount of disk space the website has used to store information on your computer, and the maximum amount of disk space the website can use before requesting additional space. The panel enables storage to be managed; if the user allows a certain website to save information on the computer, the user can limit the amount of disk space for each website by selecting 10 KB, 100 KB, 1 MB, or 10 MB. If an application needs more space than the user has allocated, a message asking for permission to use more will pop-up.

In most cases, cookies can be deleted by the user. However, the removal of the new cookies, such as Flash cookies, supercookies, etc. is not as straightforward as for regular cookies.

2.2. Cookies categorisation in terms of life span

Cookies can be categorised from their life span perspective as:

- *Non-persistent cookies, temporary cookies or session cookies.* These cookies expire when the browser is closed or when the session times out. They are usually stored in memory (cache)

- *Persistent cookies or permanent cookies.* These are usually stored at the user side in the browser memory (on the hard disk in a dedicated folder for cookies), outside of users' browser control[8]. Persistent cookies survive across multiple sessions and have an expiration date

Web servers can use both non-persistent cookies and persistent cookies. Non-persistent cookies are helpful to store status information when moving between pages of the same site; persistent cookies store information between subsequent visits. For instance, in the case of an online shop, the language/country preferences would be stored in persistent cookies, while shopping list and transactions information would be in non-persistent cookies.

6 If cookies are removed the count is not reliable anymore. Also, cookies do not always accurately identify users in cases where more than one browser is used on a computer.
7 Cookies provide the possibility to limit the number of times an ad is shown to the same user i.e. a certain popup ad appears only the first time the user visits the site. More info available at: http://www.allaboutcookies.org/ad-serving/index.html
8 Web browsers do not directly allow users to view or delete the cookies stored by a Flash application, users are not notified when such cookies are set, and these cookies never expire [6].

According to a recent ENISA survey [1], almost 80% of the online providers collect data using cookies. From the providers collecting data from cookies, more than 70% use both persistent and non-persistent cookies; non-persistent cookies are used by almost 90% of the service providers while 80% are using persistent cookies.

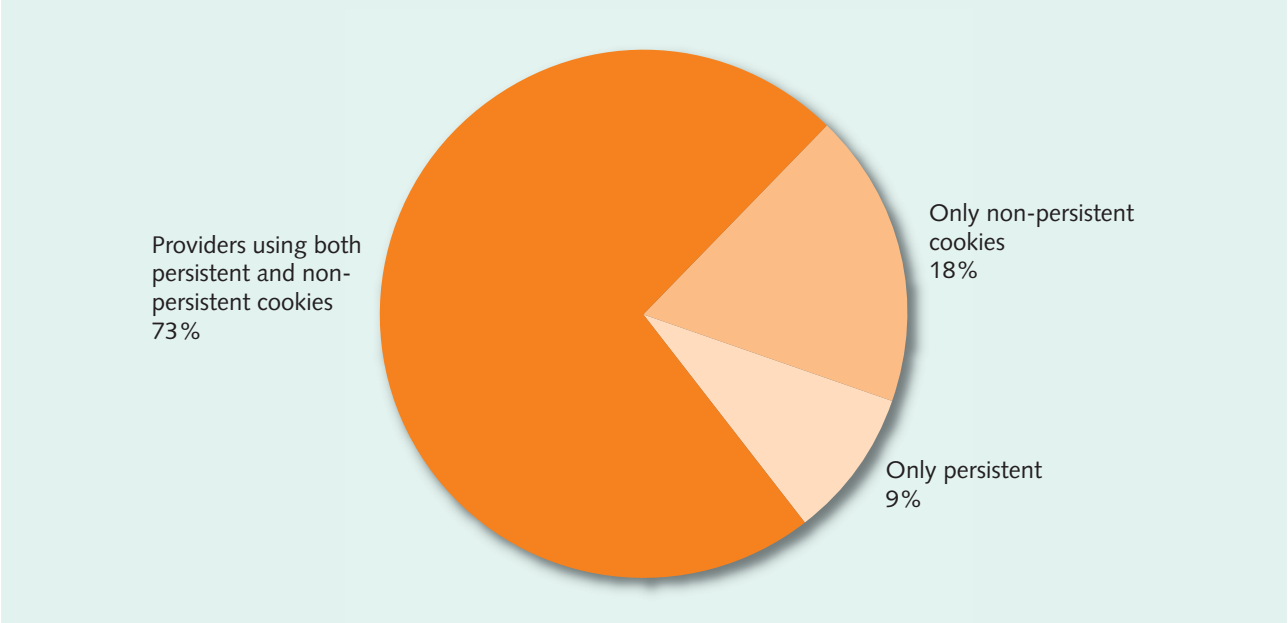

Figure 3: Online service providers using persistent and non-persistent cookies for collecting data

2.3. Cookies: removal, blocking or disabling

Commonly used browsers[9] have the ability to enable or disable cookies, or to have the browser prompt the client to accept the cookies, or not. Browsers may have built in options[10] for *private browsing and*, in such cases, cookies will not be stored. However, private browsing is not enough to guarantee privacy[11]. In fact, as demonstrated in [10], web browsers can easily be fingerprinted and are therefore identifiable to a large extent, even without using cookies.

If cookies are removed (deleted), the history of transactions between the client browser and server is deleted. As such, for the next interaction, the server considers the user as a new unique visitor.

When cookies are blocked, websites are prevented from storing cookies at the user side. Depending on the type of cookie, different situations could result:

- In the case of first party cookies, most of the convenient transactions would be impossible, i.e. to login, to remember the content of a list in an online shop and, in general, to prevent some web services from working properly
- In the case of disabling third party cookies the third party content is blocked without influencing the navigation

We note that USA.gov [11] is providing a central place for instructions on how to 'opt-out', through disabling cookies on most popular desktop browsers.

However, as mentioned previously, removing new type of cookies (i.e. Flash cookies, supercookies, evercookies) is not as straightforward, as the new cookies usually require the use of additional tools. For example, Abode provides a tool that allows a user to configure his Flash cookies [9]. Using this tool, a user can modify the storage settings, or even delete the Flash cookies associated to a site. IAB (The European trade association of the digital and interactive marketing industry) provides instructions to access cookies settings preferences for different browsers, as well as links for tools managing Flash cookies[12].

9 i.e. Internet Explorer, in Description of cookies, Microsoft support, last visited October 2010, available at: http://support.microsoft.com/kb/260971.
10 i.e. Mozilla Firefox support, Private browsing, last visited October 2010, available at: http://support.mozilla.com/en-us/kb/private+browsing
11 A tool design for anonymous browsing is FoxTor (this is a Firefox extension relying on Tor; more details about Tor and context are available in [2]). A description of FoxTor by Sasha Romanosky, FoxTor: Anonymous Web Browsing, 2006, is available at: http://cups.cs.cmu.edu/foxtor/FoxTor-Phase2.pdf, in general about FoxTor, FoxTor: Anonymous Web Browsing, available at: http://cups.cs.cmu.edu/foxtor/
12 IAB website: http://www.iabeurope.eu/cookies-faq.aspx

3. Security concerns

Any website can issue cookies. Furthermore, the information stored in a cookie by a website is usually coded in plain text and can be modified each time the user visits the web page. As a result, cookies can easily be retrieved (snooped) and forged.

Cookies have not been used in the past to run code (programs), or to deliver viruses to users' computers. Nevertheless, they have a number of vulnerabilities. Three types of threats to cookies have been identified in [7]: network threats, end-system threats and cookie-harvesting threats. Network threats result from the fact that cookies are transmitted in clear-text and can be replayed (spoofing) or modified during the transfer. SSL (Secure Socket Layer) can be used to protect cookies while they are communicated over the network. End-system threats relate to vulnerabilities, such as cookie information forgery and impersonation of other users. An attacker can perform a cookie-harvesting attack by impersonating a legitimate site and collecting cookies from users [7].

The rest of this section presents several examples of attacks on cookies. This list of attacks is by no means complete and is only provided to illustrate some of the security vulnerabilities related to the use of cookies.

In [12], session management vulnerabilities and attacks are presented; some of these attacks may expose cookies, while others exploit cookies' vulnerabilities to attack. Among them, are:

- *cache sniffing.* If the attacker accesses the browser or the proxy cache, the attacker could also obtain the cookie content

- *XSS cookie sniffing.* Cross-site scripting (also abbreviated as XSS) cookie sniffing occurs when a web application maliciously gathers data from a user. XSS attacks allow for account hijacking, changing of user settings, cookie theft/poisoning, or false advertising. The attacker can capture the cookie and extract data from it

In [13] a *session hijack attack* is presented. This type of attack is harmful, as it allows the attacker to collect private information and, at the same time, modify information, such as search results. This attack is used as starting point for a more powerful one, which reconstructs users' search histories stored by Google through the exploitation of application-specific cookies. In the first stage, a session is hijacked by eavesdropping on the traffic. The attack could be launched against any user connected via an unsecured channel. In the second phase, the search history is reconstructed using an inference attack (a technique used to disclose sensitive and protected information from presumably non-sensitive data) [13]. The reconstruction of history is partial (not always all information is gathered from history) and precise (what is retrieved is correct). In this study it is estimated that potential victims of such an attack are any users signed in and at the same time using other Google services (i.e. its search engine). The attack, however, is general and highlights privacy concerns raised by mixed architectures using both secure and insecure connections.

Typically, cookies do not have integrity checks and do not support authentication. *Cookie poisoning* tampers with the data stored in the cookie; the attributes of the cookie are altered before it is sent to the server [14]. Other weaknesses of cookies can also exploited; for instance persistent cookies could be used to impersonate a user for considerable period of time.

Another type of attack consists of impersonating users trying to access HTTPS (Hypertext Transfer Protocol Secure) servers [15]. This attack exploits improper HTTPS settings to maliciously logon into accounts and impersonate users (i.e. stolen cookies, which did not have the 'secure' attribute set that identifies HTTPS sessions, could be used to impersonate users). Examples of vulnerable websites (including online banking or email services) are given in [15].

Usually involved parties (browsers developers, websites developers) react quite promptly to the identification of such vulnerabilities by fixing them, or notifying users about the potential threats[11].

Solutions to overcome such attacks are proposed in most of the papers identifying vulnerabilities. However, existing solutions do not address all the security requirements at the same time; confidentiality – which protects against cookies' attributes being revealed to an unauthorised entity (i.e. during transfer or to another server), integrity – protecting against unauthorised modification of cookie, and user authentication, so that the cookie owner could be authenticated.

4. Privacy concerns[13]

One of the main sources of information used for profiling[14] comes from web tracking, i.e. tracking users across different visits or across different sites. Data collected includes the sequence of visited sites and viewed pages, and the time spent on each page. However, behavioural tracking is not allowed in cases of data that contain any personally identifiable information, such as name, address, phone number and so forth. Web tracking is mainly performed by monitoring IP addresses, and using techniques such as *cookies*, or the more powerful *supercookies* [16].

A user who visits a web site composed of different objects imported from different servers generates multiple HTTP requests to numerous servers controlled by different administrative domains. Very often a cookie is associated with each of these requests. As seen in Section 2, cookies are set by a web site server and are often used to store user preferences, or as authentication tokens to keep an authenticated session with a server. A cookie is sent back unchanged by the browser each time it accesses that web site. Therefore, it can be used by websites to track users across visits.

Cookies are sent only to the web sites that set them, or to servers in the same Internet domain. However, a web page may contain images, links, web bugs[15], HTML IFrame, javascript, or other components stored on servers in other domains. Cookies that are set during retrieval of these components are called *third-party cookies*[16], in contrast to *first-party cookies*. Some sites, such as those belonging to advertising companies, use third-party cookies to track a user across multiple sites. In particular, an advertising company can track a user across all pages where it has placed advertising images or web bugs. Knowledge of the pages visited by a user allows the advertising company to target advertising at the user's presumed preferences.

Note that first-party cookies are sometimes useful; they allow users to visit a site without having to re-enter their configuration parameters. However, third-party tracking raises serious privacy concerns. These privacy threats are not hypothetical but real. The increasing presence and tracking of third-party sites used for advertising and analytics has been demonstrated in a longitudinal study [17, 18]. This study showed that the penetration of the top 10 third-parties grew from 40% in 2005 to 70% in 2008, and to over 70% in September 2009. Another study shows that not only are these third-parties increasing their tracking of users, but that they can now link these traces with identities and personal information via online social networks [19]. In [20], a behavioural targeting study was performed on an e-commerce site for a clothing line. The results for the analysed case showed that the web site contained a total of nine tracking tags that linked to eight third-party companies[17]. Javascripts are also used to collect users' information. Web sites often contain executable JavaScript files that are downloaded by visiting users. These files, in addition to their computations, sometimes update first-party cookies and send information back to the servers. Javascripts have limited access to user data. However, they can access information stored in the browser, including cached objects and the history of visited links. Along with cookies and the results of JavaScript execution, the tracking sites have all the regular information available in a typical HTTP request: sender's IP address, user-agent software information, current and previous URL (via referer header), email address (from header), language preference (Accept-Language header), etc.

Supercookies and evercookies. The use of tracking cookies is ubiquitous to a large extent and there are known techniques for avoiding them [22]. This generates a big impetus in the Internet tracking industry to discover and deploy more robust tracking mechanisms, often referred to as *Supercookies* [16]. One of the most prominent supercookies is the so-called "Flash cookie", a type of cookie maintained by the Adobe Flash plug-in on behalf of Flash applications embedded in web pages [6]. Since these cookie files are stored outside the browser's control, web browsers do not directly allow users to control them. In particular, users are not notified when such cookies are set, and these cookies never expire. Flash cookies can track users in all the ways traditional HTTP cookies do, and they can be stored or retrieved whenever a user accesses a page containing a Flash application.

13 This section is based on the contribution of Claude Castelluccia to the ENISA study [2].
14 More details about Behavioural Tracking and Profiling on the Internet in the [2] ENISA report. This section has been provided by Claude Castelluccia, INRIA.
15 A web bug (also called web beacon) is a graphics on a web page or in an email message that is designed to monitor who is reading the web page or email message. Definition from EFF, The Web Bug FAQ, 1999, available at: http://w2.eff.org/Privacy/Marketing/web_bug.html
16 Some sites included JavaScript code and third-party cookies from more than ten different tracking domains [21]
17 The largest third-party ad-network companies include Advertising.com, Tacoda, DoubleClick and Omniture. Most of these networks are owned by Google, Yahoo, AOL or Microsoft. Since ad-networks are typically partnered with many publishers, they can track users across several publishers and build their browsing profiles.

These Flash cookies are extensively used by popular sites, often to circumvent users' HTTP cookie policies and privacy preferences. For example, it was found that some sites use HTTP and Flash cookies that contain redundant information [5]. Since Flash cookies do not expire, sites might automatically re-spawn HTTP cookies from Flash ones if they are deleted.

The persistence of Supercookies can be further improved, as the emergence of evercookies demonstrates [23]. This new type of cookie identifies a client even when standard cookies, Flash cookies, and others have been removed. This is accomplished by storing the cookie material in several types of storage mechanism that are available on the local browser.

5. Policy perspective

5.1. EU context

As described in *Data protection in the electronic communications sector* [24] summary of legal framework, cookies are also addressed in the context of the relevant EU policy framework. Directive 2002/58/EC [25] concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) addresses the use of cookies. This Directive contains provisions that are crucial to ensuring that users can trust the services and technologies they use for communicating electronically. The main provisions apply to spam, ensuring the user's prior consent ("opt-in"), and the installation of cookies.

In the preamble, there is reference to cookies: "*(25) However, such devices, for instance so-called "cookies", can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions. Where such devices, for instance cookies*[18]*, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC*[19] *about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. This is particularly important where users other than the original user have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment. Information and the right to refuse may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose."*[20]

Directive 2009/136/EC [26] amending previous directives, including Directive 2002/58/EC, states in its preamble:

"(66) Third parties may wish to store information on the equipment of a user, or gain access to information already stored, for a number of purposes, ranging from the legitimate (such as certain types of cookies) to those involving unwarranted intrusion into the private sphere (such as spyware or viruses). It is therefore of paramount importance that users be provided with clear and comprehensive information when engaging in any activity which could result in such storage or gaining of access. The methods of providing information and offering the right to refuse should be as user-friendly as possible. Exceptions to the obligation to provide information and offer the right to refuse should be limited to those situations where the technical storage or access is strictly necessary for the legitimate purpose of enabling the use of a specific service explicitly requested by the subscriber or user. Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application. The enforcement of these requirements should be made more effective by way of enhanced powers granted to the relevant national authorities."

18 Underlined by the authors of the paper.
19 Directive 95/46/EC is under review. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
20 Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [25]

The articles of the two directives are introduced below for comparison purposes.

Amended article 5 from Directive 2002/58/EC:

"3. Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user."

Vs. Directive 2009/136/EC Article 5(3) replaced by:

"3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service."

The amended version of the Directive[21] states that users must give their consent for information to be stored on their terminal equipment, or that access to such information may be obtained. In order to do this, users must receive clear and comprehensive information about the purpose of the storage or access. These provisions protect the private life of users from malicious software, such as viruses or spyware, but also apply to cookies.

The Directive encourages the use of methods, which are as user-friendly as possible and effective technical tools **[24]**.

There is an exception if the cookie is absolutely necessary for the provision of a service that has been requested by the user, or if information storage is for the sole purpose of carrying out an online communication. Thus, websites that carry advertising require users' consent for the provision of cookies and the same rule applies to websites that count the number of visitors[22].

As can be seen from the reactions of stakeholders regarding consent for cookies, a number of issues need clarification:

- Article 29 Working Party through **[27[23]]** already addressed certain issues, such as whether the browser settings will constitute a valid consent or not; consent in bulk for any future processing without knowing the circumstances of each processing cannot be considered valid consent. Solutions are proposed for browsers or any other application to be able to attain valid consent. Other opinions[24] have been expressed by the media on this topic

- The consent requirement relates only to cookies that collect personal data; however some cookies appear to fall outside the consent requirement[25]. The specific reference to the EU Data Protection Directive (95/46/EC) is important because it limits the consent requirement only to cookies storing personal data, as opposed to other types of information. In the opinion of the Article 29 Working Party, as well as of many data protection authorities throughout the EU, persistent cookies containing a unique user ID are personal data and therefore subject to applicable data protection rules. Arguably, some cookies (or similar technologies) may not meet these criteria and therefore fall outside the scope of the law

21 Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [26]

22 JISC Legal, EU Cookie Directive - Directive 2009/136/EC, available at: http://www.jisclegal.ac.uk/ManageContent/ViewDetail/tabid/243/ID/1347/EU-Cookie-Directive--Directive-2009136EC.aspx

23 Article 29 Working Party, Opinion 2/2010 on online behavioural advertising [27]

24 Other opinions are that the control settings in a browser or specific control panels (for Flash cookies) are sufficient to comply with the consent requirement. Such an opinion is presented by Peter Fleischer, Google Global Privacy Counsel, in The new rules for cookies in Europe, 2010, available at: http://peterfleischer.blogspot.com/2010/02/new-rules-for-cookies-in-europe.html

25 HL Chronicle of Data Protection, EU ePrivacy Directive and Cookies: The Consent Requirement May Not Be as Broad as Believed, 2009, available at: http://www.hldataprotection.com/2009/11/articles/international-compliance-inclu/eu-eprivacy-directive-and-cookies-the-consent-requirement-may-not-be-as-broad-as-believed/

- Due to national adaptation, the Member States will have the chance to clarify and/or specify some of the aspects of the Directive 2009/139/EC - or not. As suggested in the media[26] the UK could 'copy-paste' the text of the directive into national law. Any restrictive interpretation in a Member State's legislation, which would differ from other Member States, would have an economic impact on users and providers

The Member States of EU are requested to transpose into their national laws the Directive [26] 2009/136/EC by 25 May 2011. At the time of writing this paper, according to EUR-Lex[27], only Estonia, Italy and Luxembourg have prepared national execution measures. In this respect, an overview study of nationally implemented measures addressing cookies could be carried out after the transposition deadline.

Transfer of personal data outside the EU. In the ENISA study on mechanisms used in the online environment for privacy, trust etc. **[1]**, we noticed that personal data of users is transferred outside the EU, by almost half (45.5%) of the companies surveyed; the transfer is carried out in accordance with legal requirements for such transfers i.e. safe harbour. (A similar percentage (48%) of companies has been sharing users' personal data with third parties and use personal data collected for one service also to provide other services (52%).) However, outside the EU, even using safe harbour agreement, the levels of protection and the enforcement are different. In a recent publication[28] some issues are raised regarding the use of cookies by non-EU based websites.

5.2. Recent developments beyond the EU

In 2000 the United States Government Office of Management and Budget (OMB) published a new memorandum addressing federal cookie policy **[28]** with the purpose of protecting the privacy of Americans. The federal cookie policy limited the use of persistent cookies by federal agencies. Nevertheless, the prohibition of cookies was not always respected; as media coverage showed, some agencies have been using them[29].

In 2009 OMB initiated a re-examination of the cookie policy, as part of this Open Government Initiative, in the attempt to find a balance between citizen privacy and the benefits of persistent cookies. An open call for revision of the *Policy on Web Tracking Technologies for Federal Web Sites* has been published in Federal Register, in July 2009 **[29]**. Comments have been requested addressing a three-tiered approach to the use of web tracking: single-session technologies, multi-session technologies for use in web analytics and multi-session technologies as persistent identifiers. The choice between opt-in and opt-out for users, as well as the requirements for the use of new technologies, have been placed under discussion.

In June 2010, after the open consultation,two memorandums were published: *Guidance for Online Use of Web Measurement and Customization Technologies* **[30]** *and Guidance for Agency Use of Third-Party Websites and Applications* **[31]**, which modify the guidance framework by withdrawing previous restriction / guidelines (i.e. **[28]**) and stating the appropriate use and prohibitions, usage tiers, clear notice on personal use, data safeguarding and privacy, data retention limitations and access limitations. General requirements for using embedded applications and for third-party policies evaluation/examination, as well as requirements for privacy impact assessment and public notice, are included.
Following the update of guidance on how US Federal agencies can use web measurement and customisation technologies, such as persistent cookies, from June 2010, a webpage **[11]** has been published in which the instructions for 'opting-out' are provided (i.e. for each of the most popular desktop browsers and mobile browsers the steps for disabling cookies on the web browser are presented.)

In 2002, the Canadian Treasury Board issued guidelines for the use of cookies on Government of Canada websites. According to the guidelines **[32]**, an alternative should be available for visitors who do not wish to access Government of Canada Web pages with cookies. The visitors should be able to obtain the government service in some other way,

26 OUT-LAW.COM, in The Register, UK passes buck on Europe's cookie law with copy-paste proposal, You sort it out, 2010, http://www.theregister.co.uk/2010/09/17/eu_cookie_law/print.html
27 EUR-Lex, NATIONAL PROVISIONS COMMUNICATED BY THE MEMBER STATES CONCERNING: Directive 2009/136/EC, last visited January 2011, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:72009L0136:EN:NOT
28 By refusing a cookie, the user deprives himself of the protection granted by the provisions of the Data Protection directive, removing the protection shield of national data protection law, according to: "Facebook and its EU users –Applicability of the EU data protection law to US based SNS", by Aleksandra Kuczerawy, presented at PrimeLife summer school, presentation available at: http://www.cs.kau.se/IFIP-summerschool/summerschool2009/Summerschool_presentations/PrimeLife_SummerSchool_Kuczerawy_09.09.pdf
29 Cookies have been placed despite federal ban, and then removed when this has been noticed, according to The Associated Press, Spy Agency Removes Illegal Tracking Files, 2005, available at: http://www.nytimes.com/2005/12/29/national/29cookies.html

i.e. providing duplicate online access that does not use cookies, or informing visitors how they can obtain the same services through another service channel, such as a toll-free phone number, in person, fax and direct mail (if no online alternative is reasonably available).

At the end of October 2010, The Office of the Privacy Commissioner of Canada published for comments a *Draft Report on the Consultation on Online Tracking, Profiling and Targeting and Cloud Computing* [33]. The purpose of the consultation was to identify and analyse the evolving technological trends from a privacy perspective. Among the conclusions of the reports are the following: the *Personal Information Protection and Electronic Documents Act (PIPEDA)*, published in 2000, can handle the evolving technological environment. However defining what is (or is not) personal information, (determining whether cookies are personal information), determining the appropriate form of consent, limiting the use of personal information, implementing reasonable safeguards, providing access and correction, and ensuring accountability have been mentioned as issues that need careful attention. Online tracking, profiling and targeting are still largely invisible to most individuals and, according to the report, greater transparency is needed for the benefit of individuals and to ensure innovation.

The lack of visibility with respect to cookies and other tracking and profiling means can also be noticed in a study published in December 2009 [34] by the Public Interest Advocacy Centre, which surveyed Canadian consumer attitudes towards tracking. Half of the interviewed citizens, with internet access, were not familiar with cookies or web beacons (31% not at all familiar, 19% not very familiar), while 30% declared themselves somewhat familiar and 20% very familiar. We do not have reason to believe that in Europe the level of awareness is significantly higher. As such, transparency in this filed should be encouraged.

6. Concluding remarks

In this paper we identify and briefly present some of the most common types of cookies used on the Internet. Cookies were originally designed to provide answers to some technical requirements regarding state management in the interactions between users' browsers and web servers, while subsequently their use has been extended for other purposes, such as advertising management, profiling, tracking etc. The main objective of this paper is to highlight some of the security and privacy concerns generated by the use of cookies[30].

The advertising industry has already influenced the cookies development process and is supporting the development of more persistent, transparent[31], and powerful cookies. As the new types of cookie support user identification in a persistent manner, these privacy-invasive marketing practices need greater scrutiny. More research is required to reveal whether such cookies are also being used to track users; the level of identification provided should be clarified as well.

Due to privacy implications, the legal framework should be respected. However, this does not seem always to be the case. The provisions for informed consent should guide the design of systems using cookies. Users must be able to find out how a web site plans to use the information from the cookie and should be able to choose whether or not those policies are acceptable. Both the user browser and the origin server must assist in gaining informed consent. As we noticed during the preparation of this paper, in most cases users cannot easily manage cookies. This is particularly true for new type of cookies that are not controlled by browsers and require additional management tools.

Furthermore, the operation these new cookies is not well documented. For a user with limited IT expertise there is not enough information available to explain cookies' management. All cookies should have removal mechanisms that are easily used by any user; the storage of these cookies outside browser control should be limited or prohibited. In this paper we have included references where explanations are given on how cookies can be managed.

Applications and browser developers should do more to let users control how they are being tracked. However, this is not an easy task since, as shown previously, some of these tracking cookies, such as Flash cookies, are stored beyond the control of the browsers. Clearly, there is a lot of work to be done to bring these next-generation cookies even to the same level of visibility and control that users experience with regular HTTP cookies.

30 More information and findings focusing on general privacy features, online profiling etc. can be found in two new studies that ENISA finalized at the end of 2010. In the study [1] analysis of online service models is carried out to evaluate the mechanisms for obtaining informed unambiguous user consent for the disclosure of personal data. Findings of this analysis will lead to recommendations targeting users, services designers and policy makers and will be available in [2].

31 European Advertising Industry Association Condemns Cookie Re-Spawning, Lucian Constantin, October, 2010, available at: http://news.softpedia.com/news/European-Advertising-Industry-Association-Condemns-Cookie-Re-Spawning-159824.shtml and EU has trouble digesting new law on Internet Cookies - IAB Europe offers solution, available at: http://www.iabeurope.eu/news/eu-has-trouble-digesting-new-law-on-internet-cookies.aspx

Currently, for most of the services provided online, users do not have too many options at their disposal. Either they do not accept cookies and therefore cannot access to the service, or they accept cookies, with all the consequences related to privacy and security. The users should be able to have access to services, providing they do not accept cookies through another service channel.

From a policy perspective in the EU, a new Directive has to be transposed in Member States' national legislation. The terms regarding cookies and similar techniques are not always straightforward. This can generate discussions and differences in interpretation for users and providers. However, the new legal context underlines the need for a valid consent, expressed by the user, providing prior clear and comprehensive information provided for the user.

As mentioned in Section II.4, the Member States of the EU are requested to transpose into their national laws the Directive 2009/136/EC by 25 May 2011 [26]. As a first step, an overview study of the measures implemented at Member States' level addressing cookies could be carried out after the transposition deadline.

7. Acknowledgments

The authors would like to express their gratitude to the members of the ENISA Expert Group on Privacy Accountability and Trust: Simone Fischer Hübner (Karlstad University, Sweden), Claude Castelluccia (INRIA, France), Peter Druschel (Max Planck Institute for Software Systems, Germany), Aljosa Pasic (Athos Origin, Spain), Bart Preneel (K.U.Leuven, Belgium) and Hannes Tschofenig (NSN, Finland) for their contributions for ENISA report [2], which was the starting point for this paper. Michelle Chibba (IPC, Ontario, Canada) provided useful links on recent Canadian developments regarding cookies. We would like to express our gratitude for the valuable comments received from: Slawomir Gorniak, Ulf Bergstrom, Steve Purser, Udo Helmbrecht, Panagiotis Saragiotis, and anonymous reviewers.

8. References

[1] ENISA, Survey of accountability, trust, consent, tracking, security and privacy mechanisms in online environments, 2010, available at: https://www.enisa.europa.eu/act/it/library

[2] ENISA, Privacy, accountability and trust – challenges and opportunities, 2010, to be available at: https://www.enisa.europa.eu/act/it/library

[3] David Kristol, HTTP Cookies: Standards, privacy, and politics, ACM Transactions on Internet Technology, 1(2), 2001, pp.151–198, available at: http://www.cs.stevens.edu/~nicolosi/classes/sp10-cspriv/ref5-1.pdf

[4] IETF RFC 2965, HTTP State Management Mechanism, published in 2000, available at: http://www.ietf.org/rfc/rfc2965.txt

[5] Soltani Ashkan, Canty Shannon, Mayo Quentin, Thomas Lauren, and Jay Hoofnagle Chris, Flash cookies and privacy, Technical report, University of California, Berkeley, 2009, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862

[6] Seth Schoen, EFF, New Cookie Technologies: Harder to See and Remove, Widely Used to Track You, September, 2009, available at: http://www.eff.org/deeplinks/2009/09/new-cookie-technologies-harder-see-and-remove-wide

[7] Joon Park, Ravi Sandhu, Secure Cookies on the Web, IEEE Internet Computing, July-August, 2000, pp. 36-44.

[8] Microsoft MSDN, userData Behavior, last visited November 2010, available at: http://msdn.microsoft.com/en-us/library/ms531424%28VS.85%29.aspx

[9] Adobe Flash Player Help, Documentation, Website Storage Settings panel, available at: http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager07.html

[10] Eckersley Peter, How unique is your web browser?, in Proceedings of the 2010 Privacy Enhancing Technologies Symposium (PETS), 2010, LNCS 6205, pp1-18.

[11] USA.gov, Web Measurement and Customization Opt-out, 2010, available at: http://www.usa.gov/optout_instructions.shtml

[12] C.A. Vlsaggio, L.C. Blasio, Session Management Vulnerabilities in Today's Web, IEEE Security & Privacy, Vol.8, Issue 5, Sept.-Oct. 2010, pp.48-56.

[13] Claude Castelluccia, Emiliano De Cristofaro, Daniele Perito, Private Information Disclosure from Web Searches (or how to reconstruct users' search histories), in Proceedings of the 2010 Privacy Enhancing Technologies Symposium (PETS), 2010, LNCS 6205, pp. 38-55.

[14] G. Pujolle, A. Serhrouchni, I. Ayadi, Secure session management with cookies, in:Proc. Of 7th International Conference on Information, Communications and Signal Processing (ICICS), 2009, 6 pages, available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5397550

[15] Shuo Chen, Ziqing Mao, Yi-Min Wang, Ming Zhang, Pretty-Bad-Proxy: An Overlooked Adversary in Browsers' HTTPS Deployments, in: proc. of 30th IEEE Symposium on Security and Privacy, 2009, pp. 347 – 359, available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5207655

[16] Katherine McKinley, Cleaning up after cookies, Technical report, iSEC PARTNERS, December, 2008, 12 pages, available at: https://www.isecpartners.com/files/iSEC_Cleaning_Up_After_Cookies.pdf

[17] B. Krishnamurthy and C. Wills. Privacy diffusion on the web: a longitudinal perspective. In WWW '09: Proceedings of the 18th international conference on World wide web, ACM, 2009.

[18] B. Krishnamurthy and C. Wills. Privacy diffusion on the web: a longitudinal perspective (updated graphs), September 2009, available at: http://www.ftc.gov/os/comments/privacyroundtable/544506-00009.pdf

[19] B. Krishnamurthy and C. Wills. On the leakage of personally identifiable information via online social networks. In WOSN '09: the second workshop on Online social networks, 2009.

[20] Catherine Dwyer. Behavioral targeting: A case study of consumer tracking on levis.com, in Fifteen Americas Conference on Information Systems, 2009, available at: http://www.ftc.gov/os/comments/privacyroundtable/544506-00046.pdf

[21] Peter Eckersley, EFF, How Online Tracking Companies Know Most of What You Do Online, 2009, available at: https://www.eff.org/deeplinks/2009/09/online-trackers-and-social-networks

[22] Pam Dixon, World Privacy Forum, Consumer tips: How to opt-out of cookies that track you, 2009, available at: http://www.worldprivacyforum.org/cookieoptout.html

[23] Evercookie–never forget, available at: http://samy.pl/evercookie/

[24] EUROPA.EU, Data protection in the electronic communications sector, legislation summary, 2010, available at: http://europa.eu/legislation_summaries/information_society/l24120_en.htm

[25] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), last visited November 2010, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:NOT

[26] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, last visited November 2010, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009L0136:EN:NOT

[27] Article 29 Working Party, Opinion 2/2010 on online behavioural advertising, 2010, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

[28] US Office of Management and Budget, M-00-13, Privacy Policies and Data Collection on Federal Web Sites, June, 2000, available at: http://www.whitehouse.gov/omb/memoranda_m00-13

[29] US Office of Management and Budget, Proposed Revision of the Policy on Web Tracking Technologies for Federal Web Sites, in US Federal Register, Vol. 74, No. 142, July, 2009, available at: http://edocket.access.gpo.gov/2009/pdf/E9-17756.pdf

[30] US Office of Management and Budget, M-10-23, Guidance for Agency Use of Third-Party Websites and Applications, June, 2010, 9 pages, available at:
http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf

[31] US Office of Management and Budget, M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies, June, 2010, 9 pages, available at:
http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-22.pdf

[32] Canadian Treasury Board, Guidelines for Cookies on Government of Canada Web Sites, 2002, available at:
http://www.tbs-sct.gc.ca/pgol-pged/cookies-temoins/cookies-temoins-eng.rtf

[33] Office of the Privacy Commissioner of Canada, Draft Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting and Cloud Computing, October 2010, available at: http://www.priv.gc.ca/resource/consultations/report_2010_e.cfm

[34] Public Interest Advocacy Centre, Tracking Consumers Online – Behavioural Targeted Advertising and a "Do Not Track List" in Canada, December 2009, available at: www.piac.ca/files/dntl_final_website.pdf

PO Box 1309 71001 Heraklion Greece
Tel: +30 2810 391 280 Fax: +30 2810 391 410
Email: info@enisa.europa.eu
www.enisa.europa.eu