Issues in Informing Science and Information Technology Volume 5, 2008

# Online Privacy Analysis and Hints for Its Improvement

*Tanja Krunić and Ljiljana Ružić-Dimitrijević*
*The Higher Education Technical School of Professional Studies, Novi Sad, Serbia*

ljaga@eunet.yu; krunic@nspoint.net

## Abstract

The idea of the paper is to investigate how much the online user privacy is respected by website owners, and how online privacy can be improved. We first focus ourselves on issues like possibilities of misusing personal data, data collecting and user-tracking. Then we give a short report about legislation in the EU concerning user privacy.

Some facts about user confidence are given as well. They are follows by a brief list of hints for the users to protect their personal data when surfing the Web. Then we give an overview of actions website owners should take in order to support user privacy. Finally, we present the results of our investigation of the condition of user privacy in practice, and give some suggestions on its improvement.

**Keywords:** privacy, website, misuse, web design, user.

## Introduction

Twentieth century technology provides various communication means. The Internet is a powerful interactive and multimedia communication medium offering numerous activities. Many companies utilize the Internet for the enlargement of their business. They create websites for advertising, contact information, e-shopping, etc.

Modern people use the Internet for diverse purposes such as information, education, entertainment, e-shopping, etc. All these services are useful, but at the same time can be misused, as well.

There are a lot of cases of misuse, from malicious scripts causing various types of damage on user's hardware or software, to jeopardizing personality by misusage of personal data. The Internet users have very soon become aware of the risk of the Internet usage. They are worried, sometimes unnecessarily, but sometimes with a reason.

Today almost every computer is equipped with some antivirus software providing several levels of protection. Complete protection is impossible because of the expanding skills of virus authors; still users may improve safety by acquiring new and updating current antivirus software.

Regarding personality protection, users are not often aware of the danger, and ways of collecting their personal data. In many cases they do not sense the jeopardy, since personal data are not given directly. Websites can collect such data in different ways, without user's knowledge, and sometimes the user is compelled to provide own personal data in order to perform an activity on the Web.

Website visitors may improve their personal safety by recognizing possibilities of misusing personal data and how they can protect themselves. In addition, there is a set of recommendations given by W3C organization about many web issues and one of them is the user's privacy.

## Possibilities of Misusing Personal Data

Surfing the Web people are daily asked to fill out forms dealing with their personal data. They are mainly asked about their name, family name, home address, telephone number, date of birth, hobby, profession, business, loan, credit card number, etc. Unfortunately, there are numerous possibilities of misusing someone's personal data. We will mention several of them:

- **Spam**. Sending undesired e-mails is a very common misuse of personal data. Companies use data collection and user tracking for finding out user habits and interests, which can be misused for sending spam. Moreover, companies often share collected personal data with other companies. For example, ("Privacy matters", 2001) the Double Click company claimed in January 2000 to exchange collected personal data with the Abacus Direct Company. The same source mentions also some companies with financial problems that tried to sell their personal data collection in order to survive on the market, like Toysmart.com in June 2000. Fortunately, the above mentioned company renounced the data selling, after solving their financial problems in another way.
- **The misuse of credit card numbers**. Credit card numbers can be misused after security incidents. Such incidents happened for example, in 2000 at CreditCards.com, Eve.com and Amazon.com. An investigation made by Gartner and Harris Interactive, shows that among 1.000 adult online users in a period of 12 months, there were 7% of victims related to a credit card information misuse, (Knowledge Leader, 2006). One of several methods for credit card misuse is known as spoofing. Namely, criminal groups clone entire websites or their parts concerning credit card information and product purchasing, assuring clients to be the very legal website of a trademark company. They mainly offer products at a significantly lower price then the usual, which is an additional motive for people to purchase products at the false online store. After the collection of credit card information, the deceived clients are e-mailed about the successful transaction, so the clients can hardly understand they are misused. Clearly, there are many more types of credit card frauds; we do not aim to mention them all in this paper. For additional information about methods of credit card misuse, we refer to (Simovic, 2006).

  However, an annual analysis of the National Information Center-a (NIC) for 2005 year, ("Internet scams fraud trends," 2005) claims that the amount of registered credit card misuses in 2005 values $13.863.003.
- **Crime.** Personal data collectors can sell personal data to criminal groups. Such an example is mentioned in ("Privacy matters," 2001). After buying jewelry online, the client's personal data was sold to a criminal group which robbed the person several days later. Another example is about a teenager who used the Web to find out the address of a girl he liked in order to kill her (Powell, 2000).
- **Secret services.** It is well known that the FBI in the USA owns a user tracking system DCS1000 ("Privacy matters", 2001). That system is installed at Internet providers in order to track suspected people under investigation. Groups for privacy protection are concerned about misusing the system for tracking unsuspected people as well.

## *Data Collection and User Tracking*

Let us explain the most common ways of data collection and user tracking.

- **Forms** refer to the main data collector present at almost all on-line stores. Before purchasing products, users are asked to fill out forms with data including name, credit card number, age, address, etc.

- **Forms using *get*.** There are two form submission methods: post and get. In the case of using the get method of form submission, the web browser attaches the submitted data to the web server URL, and the web server places it into the Request collection. However**,** the get method of form submission is known for its privacy vulnerabilities (Jamsa, King, & Anderson, 2002); since the submitted data can be read from the URL address. Unfortunately, web designers use the get method frequently, since it is widely web-browser supported. Nevertheless, it is more secure to use the post method of form submission, since the web browser sends the submitted data through the head of the HTTP message. Then the data is seen by the web server as a part of the Request.Form collection. Unfortunately, this method is not supported by all web browsers, so it is less used than the get method.

- **Cookies.** Cookies are text files stored on users' computers. Websites use them to collect information for their own purpose. Cookies can be described like placeholders that indicate one has already visited a web page or remember the users' preferences. Such cookies are harmless, since they only contain information meant for users' benefit. However, some companies use cookies to track users' behavior on the Web, depending on whether the cookie is a first party or third party cookie.

- **First party cookies** either originate on or are sent to the website a user is currently viewing. These cookies are commonly used to store information, such as preferences when visiting that site.

- **Third party cookies** are not set by the visited website, but rather by a site on another location. This is the case with most advertising banners. There are also companies that readily abuse the technology in order to track web surfers all over the Internet. One such company is advertising giant DoubleClick, (www.doubleclick.com). **DoubleClick** is a company that develops and provides Internet advertising services (technology and service that place advertisements on websites). Its clients include agencies, marketers (Universal McCann Interactive, AKQA etc.) and publishers that serve customers like Microsoft, General Motors, Coca-Cola, Motorola, L'Oreal, Palm, Inc., Visa USA, Nike, Carlsberg among others. (For more information see DoubleClick, 2007). However, cookies are designed to be accessible only by the site that sets them. DoubleClick is said to exploit a loophole by running ad banners from its own servers, and using those servers to set and read cookies, see ("Cookies," 2005). DoubleClick has ads on thousands of websites and can read any cookie set by any of them. So DoubleClick uses these cookies to track web surfers from one website to another.

- **Web beacons.** Generally, a web beacon ("What is a web beacon?" 2005) consists of a small string of codes that represents a graphic image request on a web page or e-mail. There may or may not be a visible graphic image associated with the web beacon and often the image is designed to blend into the background of the web page or e-mail. Web beacons may be delivered from the same or from different domain than the web page or e-mail viewed. They may be used by the party responsible for the web page or e-mail viewed (first-party web beacons) or by the third-party (third-party web beacons).

- **Third party links** are links connecting the visited website with a website not currently viewed.

## Legislation

The Internet user privacy in the European Union relies on the Directive 2002/58/EC of The European parliament concerning the processing of personal data and the protection of privacy in the electronic communications sector. The document points to the Internet as a service that opens new possibilities for users, as well as new risks for their personal data privacy. It also obligates all member states to provide specific legal, regulatory and technical provisions in the case of public communication networks, in order to protect fundamental rights and freedom of natural persons and legitimate interests of legal persons, in particular with regard to the increasing capacity for automated storage and processing of data relating to subscribers and users. Also, those regulatory and technical provisions adopted by the member states concerning the protection of personal data, privacy and the legitimate interest of legal persons, in the electronic sector should be harmonized in order to avoid obstacles to the internal market of electronic communication. Harmonization should be limited to requirements necessary to guarantee that promotion and development of new electronic communications services and networks between Member States are not hindered. In the following section we provide details of several aspects of the Directive; for more details see Directive 2002/58/EC (2002).

The prohibition of storage of communications and the related traffic data by persons other than the users or without their consent is not intended to prohibit any automatic, intermediate and transient storage of this information in so far as this takes place for the sole purpose of carrying out the transmission in the electronic communications network and provided that the information is not stored for any period longer than is necessary for the transmission and for traffic management purposes, and that during the period of storage the confidentiality remains guaranteed. Where this is necessary for making more efficient the onward transmission of any publicly accessible information to other recipients of the service upon their request, this Directive should not prevent such information from being further stored, provided that this information would in any case be accessible to the public without restriction and that any data referring to the individual subscribers or users requesting such information are erased. Confidentiality of communications should also be ensured in the course of lawful business practice, particularly where necessary and legally authorized communications can be recorded for the purpose of providing evidence of a commercial transaction. Directive 95/46/EC applies to such processing. Parties to the communications should be informed prior to the recording about the recording, its purpose and the duration of its storage. The recorded communication should be erased as soon as possible and in any case at the latest by the end of the period during which the transaction can be lawfully challenged.

Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned.

However, such devices, like cookies, can be a legitimate and useful tool, for example, in analyzing 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, 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 (Directive 95/46/EC, 1995) 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.

Also, European countries not being members of the European Union are making efforts in order to harmonize with the EU Directive 2002/58/EU. For example, the Serbian parliament created a law in this manner (The National Law about Advertising, 2005). The mentioned law points to the Internet as an advertising medium, and hence spam and advertising e-mails with the false identity of the sender are strongly forbidden.

## User Confidence

The authors of this paper made a short investigation about user confidence in Serbia (Krunic, 2006). Web users of different ages, sex and interests were asked questions about the importance of personal data privacy. We will give only the main results of the investigation herein. 85% of the users were concerned about others accessing their personal data. Especially if the personal data included the credit card number, 60% of them canceled the transaction. About 50% of them explained they were afraid of hackers who could get their credit card numbers. About 25% of the users did not want to share their personal data in order to avoid getting spam. Only 10% of the users did not mind sharing their personal data. We conclude that there is a low rate of user confidence in Serbia. Additionally, more than half of the users asked for a better control of the use of their personal data. On the other hand more than 30% of the users gave false personal data when filling a form to be sure that no one could misuse their personal data. It is interesting that about 40% of the users were not informed about what a privacy statement is, almost the same number of users asked for a privacy statement before entering an online shop, while about 20% of the users did not care about privacy statements.

Another investigation made on 603 Web users in the USA, Great Britain, Germany and France, (*Trends and Attitudes in Information Security*, 2006) claims that although 63% of all users feel secure during internet transactions (57% in the USA, 66% in the UK, 72% in Germany, and 71% in France), 43% of all users (41% in the USA, 45% in the UK, 30% in Germany and 57% in France) do worry about others accessing their personal data.

### *Hints for Users to Help Protecting Their Own Privacy Online*

It is obvious that there is a growing risk for the misuse of personal data through the global use of the Internet. Fortunately, users themselves can do a lot to protect personally identifiable information that is gathered about them when they surf along the Internet or enter online stores. Let us introduce some actions they can take to protect their own personal data. (For more details see “ABC’s of Online Privacy,” 2003; “Rules and Tools,” 2003; “Privacy tips,” 2003).

### Rules to remember for protecting personal privacy:

- **Look for a privacy policy** on every website that asks you to register or provide information. A credible privacy policy should be easy to find and easy to understand. Most ethical web-sites put a link to a privacy policy right on the home page. The policy should tell you exactly what information a website collects and what it is used for. If the website shares the information with anyone else it should tell you and give you the option of restricting such a use. A privacy policy also should tell you about the security used to protect your personal information and how you can look at the information that is collected about you. Nowadays, all consumer websites that treat information ethically have privacy policies. Look for them and use them and only use sites where they are provided.

- **Look for a privacy seal**. These seals, (Figure1) which are a recent innovation, give assurance that a website is abiding by its posted privacy policy. BBBOnLine (http://www.bbbonline.org/ a subsidiary of the Council of Better Business Bureaus) and TRUSTe (www.truste.org/) seals provide a mechanism to handle complaints by consumers who feel their privacy has been violated. The seals also mean a company has instituted systems for practicing what it preaches about privacy protection. Web Privacy Seal builds confidence between business and consumers by identifying business with reliable privacy practice. For example, TRUSTe's seal marks companies that adhere to TRUSTe's strict privacy principles, and comply with the TRUSTe Watchdog dispute resolution process. Principles include:
  - Creating a privacy policy to be reviewed by TRUSTe;
  - Posting notice and disclosure of collection and use practices of personally identifiable information; and

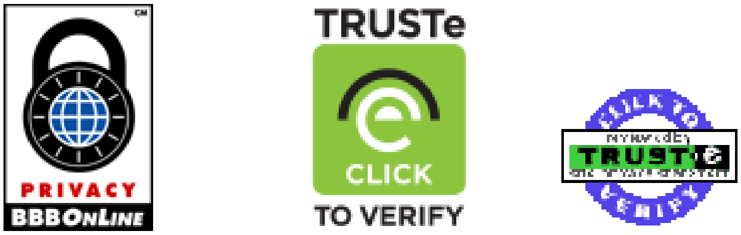

**Figure 1: Privacy seals**

  - Giving users choice and consent on how their information is used and shared.
- **Do not under any circumstances give your password to anyone**. Hackers and scammers often try to entice you to give you password through a variety of tricks. Be careful. Use different passwords at different websites and change your passwords every now and then.
- **Use a secure browser** that complies with an industry security standard, such as Secure Sockets Layer (SSL) that encrypts or scrambles purchase information.
- **Print a copy of your purchase order** and confirmation number for your records when shopping online.

## Checklist for reading a privacy policy

When reading a privacy policy, there are questions you should ask:

- What information does the company collect about me?

Everyone should know what information is collected about him/her. Websites may collect different information from users. It depends for what purpose it will be used. It may be personal information like name, e-mail, mailing address, phone number, a credit card number, etc. Sometimes questions are about your personal preferences, to learn about your needs and wishes.

- Is the information necessary for the online activity I am engaging in?

If you are ordering products online, it is understandable that your personal data (name, address, credit card number) are necessary, but not information about your preferences. This information can be collected for future market or share with others. Therefore, you can decide not to release that information.

- How does the site collect information about me?

Most websites use cookies to recognize our computer the next time we visit. They store information about domain and host from which we access the Internet, IP address of the computer, the date and time, and the Internet address from which we are linked to the website. We can deactivate cookies, but it may limit our activities in the website.

- How does the site use personal information once it is collected?

The information can be used for completing a transaction and the payment. In some cases the information can be shared with other companies, third parties, due to sending you information you may be interested in.

- Do I have a choice about the way the information about me is used or shared? How can I make that choice?

Websites mainly use portions of information to do some transaction with the user. In addition, they may use information on the user to send future offers, or share it with others. In these cases, sites have to enable a choice about whether or not they may use the information in such ways. That choice can be made by providing an opt-out box, calling a toll-free number or writing directly to the company.

- What assurances do I have that the information is protected?

Websites can use a variety of secure techniques to protect your information, like secure servers, firewalls, and encryption of financial date. If you provide personal information in chat rooms, forums, etc. in these sites, it is available to other users.

- Can I access the information collected about me?

Website should offer access to your online profile, or requesting a copy of your profile at the contact address.

- Does the website provide a place where I can take my complaints about the use of my information or have my questions and information use answered?

Some sites provide a contact where you can bring your complaints or questions about privacy.

## Products and services

The market for privacy protection products is growing and companies are responding with a host of technological tools and services. Some of these are available free and many can be downloaded. Here is a partial list of those that are available.

- **Anonymizers and infomediaries**. Tools for protecting privacy can be divided into two kinds; those that work to shield your identity and those that help you negotiate with a website over what personally-identifiable information is shared.
    - **Anonymizers** make you "anonymous" by giving you an untraceable alias. While a useful tool for some consumers, anonymizers can protect lawbreakers. (Anonymizer, www.anonymizer.com), (Crowds, www.research.att.com/projects/crowds.)

- o **Infomediaries**, a new and relatively untested technology, allow you to exercise choice in what sorts of personal information is shared at each site you visit. They require that you create a detailed personal profile to enable the technology to negotiate the release of personal information on your behalf. (**DigitalMe,** www.digitalme.com), (**Jotter,** www.jotter.com), (**Lumeria,** www.lumeria.com)

- **Secure Servers and Browsers.** Most websites offer some protection for sensitive account information, but to be safe you should shop at sites with one of two security methods: Secure Electronic Transfer Transaction or Secure Socket Layer. Both Netscape Navigator and Microsoft Internet Explorer can hook into these standards.
  - o **Secure Electronic Transfer Transaction** (SET) works by using encryption to safeguard your credit card information while it's traveling over the Web. It also uses digital signatures to ensure the identity of both you and the merchant. One advantage of SET is that your credit card number is not stored in the merchant's browser.
  - o **Secure Socket Layer** (SSL) creates a secure connection for transmitting documents and information such as credit card numbers over the Internet. It is fast and easy for websites to set up. SSL may become the accepted standard for web-based transactions that require a high degree of security.

It is easy to tell if you are using a secure site, just look for an "s" in the end of the "http" in the site's web address ("https"). The "https" will appear when you are in a frame that asks for your account information.

A recent development is **secure HTTP (SHTTP)** a secure method for transmitting individual messages, such as e-mail, over the Web. This differs from SSL and SET, which are primarily used for doing business on websites.

## Company Side of User Privacy Support

Achieving user confidence is an important issue for companies attempting to lead their business on-line. Preventing user fear about the misuse of their personal data removes all their barriers for using on-line stores. Although there are some costs for supporting user privacy, achieving user confidence widens the market which multiples the income.

In order to support user privacy, a company should place at least a privacy statement on their website. A privacy statement is a companies' declaration about what user information is collected and for what purpose.

However, a privacy statement is frequently insufficient to gain user confidence. The World Wide Web Consortium (W3C) developed the Platform for Privacy Preferences Project (P3P) (2007), creating a simple, automated way for users to have more control over the use of personal information on websites they visit. Its basic level, P3P is a standardized set of multiple-choice questions covering all major aspects of the website's privacy polices. Taken together, they present a clear snapshot of how the site handles personal information about its users. P3P enables websites to make this information available in a standard, machine-readable format. It also enables browsers to "read" this snapshot automatically and compare it to the consumer's own set of privacy preferences. P3P enhances user control by putting privacy polices where users can find them, in the form users can understand, and, most importantly, enables users to act on what they see. Any organization wishing to increase user confidence should consider implementing P3P ("Why Implement P3P?" 2002). The P3P specification brings ease and regularity to web users wishing to decide whether and under what circumstances to disclose personal information. User confidence in online transactions increases as they are presented with meaningful information and choices about website privacy practice.

However, although P3P provides a technical mechanism for helping users about privacy polices before they release personal information, it does not provide a mechanism for ensuring sites act according to their polices.

Let us introduce the aspects of online privacy covered by P3P:

- Data being tracked by the site:
  - Who is collecting the data?
  - Exactly what information is being collected?
  - For what purposes?
  - Which information is being shared with others?
  - Who are these data recipients?
- The site's internal privacy polices
  - Can users make changes on how their data is used?
  - How are disputes resolved?
  - What is the policy for retaining data?
  - Where can the detailed polices be found in a "human readable" form?

Let us explain how it works: P3P enables websites to translate their privacy practices into a standardized, machine-readable format (Extensible Markup Language XML) that can be retrieved automatically and easily interpreted by a user's browser. Translation can be performed manually or with automated tools. Once completed, simple server configurations enable the website to automatically inform visitors that it supports P3P. In Figure 2 it is presented how to make your website P3P compliant. A simple http transaction with P3P added is shown in Figure 3.

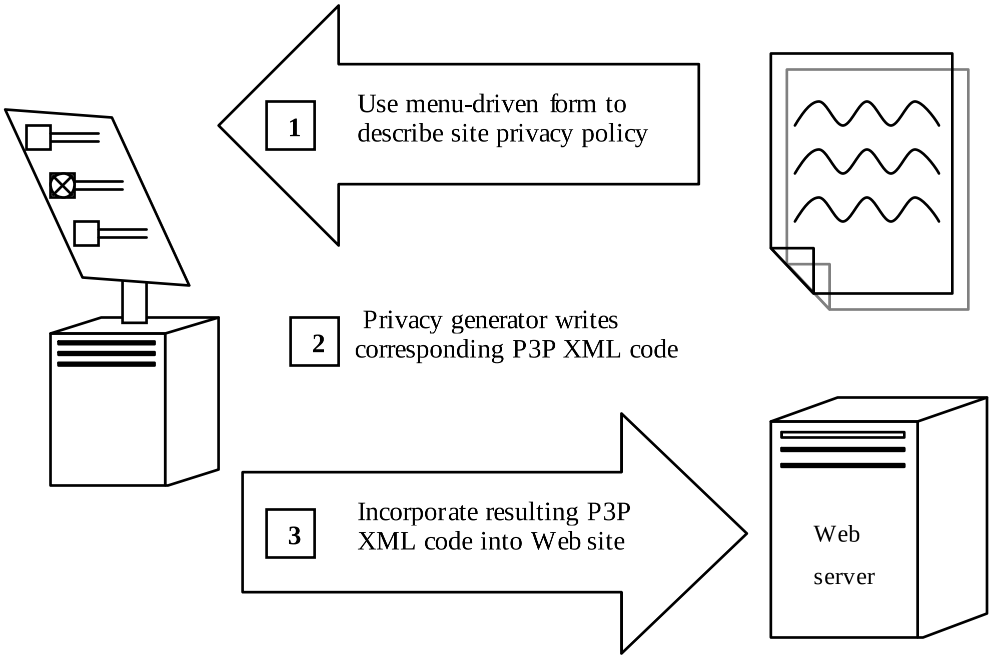
1
Use menu-driven form to describe site privacy policy
2
Privacy generator writes corresponding P3P XML code
3
Incorporate resulting P3P XML code into Web site
Web server

**Figure 2: Making your website P3P compliant**

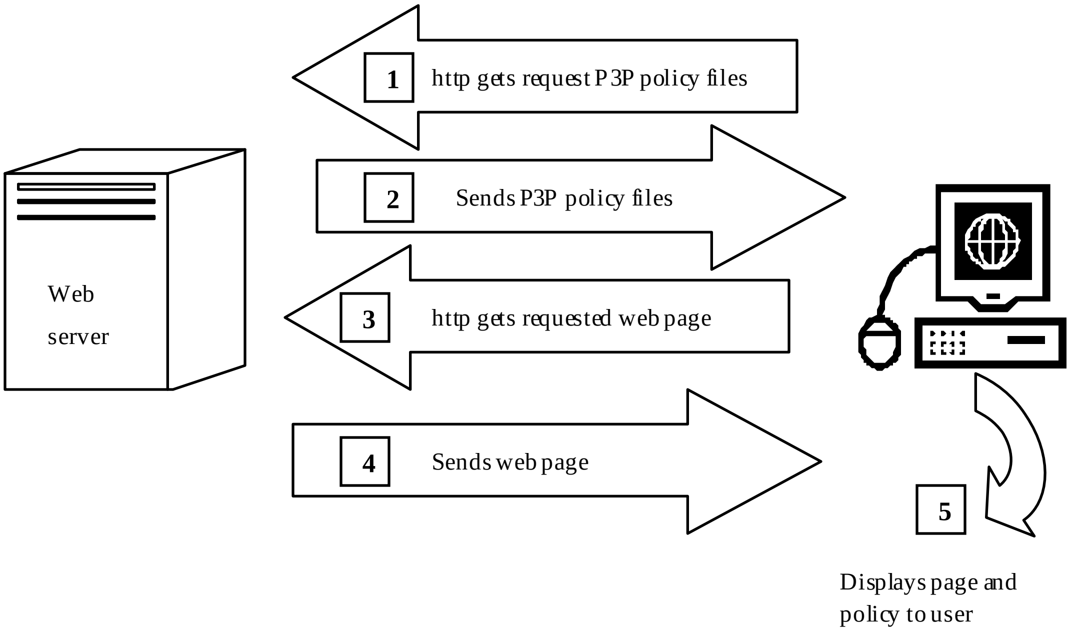

**Figure 3: A simple http transaction with P3P added**

On the user side, P3P clients automatically fetch and read P3P privacy policies in websites. A user's browser equipped for P3P can check a website's privacy policy and inform the user of the site's information practice. The browser could then automatically compare the statement to the privacy preferences of the user, self-regulatory guidelines, or a variety of legal standards from around the world. The P3P client software can be built into a web browser, plug-ins, or other software.

A very important fact for the implementation of the P3P polices is that it does not require new server software. Namely, P3P 1.0 uses the normal HTTP 1.1 protocol for the exchange of policies, and the matching of policies to user preferences takes place on the client-side. Thus, P3P can be installed in websites that use any HTTP server. Websites can implement P3P 1.0 from their servers by translating their human-readable privacy policies into P3P syntax and configuring their servers to identify the location of the P3P policy.

The P3P policies can be referred in three different ways. It is expected that many server administrators employ policy reference files in a well-known location to simplify website administration. To do this, a policy reference file (p3p.xml) need to be placed in a directory called /w3c, where /w3c is located under the root directory. A user agent can then request this file by using an HTTP GET request for the resource /w3c/p3p.xml. Alternatively, servers may be configured to insert a P3P header into an HTTP response to indicate the location of a site's P3P policy, or they can be configured to insert this information into HTML content as a LINK tag.

Another important fact is that P3P has a very low impact web performance. In most cases, the first time a user visits a website, their browser will have to make one or two additional requests in order to locate and fetch the P3P policy. These requests may impose some minimal latency; however, the delay caused by this should usually be less than the delay from fetching a single image in a web page. Subsequent requests to the same site will usually not include any additional latency due to P3P, as long as the site's policy has not expired.

What are the benefits of P3P in a regulated environment like the EU? In a regulated environment like the EU, users have certain rights. This includes not only the right to be notified when data is collected but also the right to access data under reasonable conditions, requirements for informed consent, and so on. To put these rights into effect it would be useful to have software that could help manage flows of information. P3P can help because it is an open standard, and as such could allow many different types of software to interoperate with each other on the Web ("P3P & Privacy on the Web FAQ", 2002*)*. A second benefit of P3P is that data commissioners in Europe, along with other privacy groups, could come up with recommended privacy preferences that could be shared easily and used by anyone with a P3P-enabled browser. Also, by expressing privacy statements in a simplified, structured format, P3P could assist companies in complying with the EU Data Directive, as well as help data commissioners keep tabs on companies' practices.

## Online Privacy Investigation

The aim of the authors was to detect in what range user tracking and data collecting is performed, and on the other hand, how much the privacy policy and the P3P policy platform are implemented in practice. First we will present some results from our prior investigations. These investigations indicated that companies are more familiar with user tracking and data collecting than with user privacy supporting. Namely, in Krunic, Ruzic-Dimitrijevic, Petrovic, and Farkas (2006) we used the free tool for online privacy checking for testing 50 arbitrarily chosen websites worldwide, and concluded that 32% of the checked websites were implementing some sort of user tracking or data collecting, while only 8% were using P3P. Since the checked websites were chosen from different countries, they were written in different languages, so no investigation about privacy polices was made. Similarly, in Krunic (2006) 30 online stores in Serbia were tested, and the results were as follows: 83.9% used forms, 32.2% used form with the get submission method, 42.2% used first-party cookies denied for default Internet Explorer settings (i.e. cookies using personally identifiable information without implicit consent), third-party cookies were not found, web beacons were present in 38.8% of the websites, third-party links were found in 87.1% of the websites. On the other hand, only 9.7% of the websites placed a privacy policy. The P3P policy was supported in only 2.7% of the websites.

For the purpose of this paper, we made two more detailed investigations. First, we checked 200 websites from 13 different countries (the complete list can be found in the Appendix), mainly dealing with e-commerce, since they are the websites mostly collecting data about their users, with the above mentioned Webxact online privacy check tool (http://www.webxact3.watchfire.com). Webxact has the ability to check the presence of forms, forms using the get method of submission, first-party cookies denied for the default Internet Explorer settings, third-party cookies, third-party links, and web beacons. On the other hand, it checks if the site implements the P3P platform. However, the presence of a privacy statement has to be checked manually.

Therefore, an additional research was conducted in December 2006 by the second year students of Web Design. They chose websites arbitrarily, and tried to find a privacy policy for each of them. The instruction was to compare the results from our country and foreign countries. Foreign websites are mostly in the English language. As there were several replicated websites, they were counted as one. 145 foreign and 69 domestic websites were processed in total.

Some students chose websites dealing with a specific business, like banks, technical companies (Philips, Sonny, Nokia, etc.), media (newspapers, TV and radio), and their results are very significant.

Also, they had to download privacy policy page for the purpose of investigating its content. We discussed aspects of online privacy covered by the privacy statement.

We have to underline the limitation of our research due to a small sample, and various website categories. Websites dealing with e-commerce have a higher responsibility to provide user privacy. In any case, it is obvious that domestic websites hardly support privacy.

The next limitation can be that the students included more famous foreign websites like searching engines, hardware and software suppliers, and we can suppose they have more professional web teams making an effort to incorporate W3C recommendations, including privacy policy.

## The Results of the First Investigation

As expected, e-commerce websites use forms in a high percentage. However, it is obvious from Table 1, that such websites around the world (except in Serbia and Sweden where the percentage is lower than 50% but still not insignificant) are mainly using forms with the get method of submission, which is known as vulnerable in the sense of privacy.

Table 2 shows us that cookies are mainly used for the users' benefit, since there is a low percentage of presence of either first-party cookies denied for default Internet Explorer privacy settings (except in France, India and Sweden were the percentage is a little higher, but still lower than 50%) and third-party cookies. On the other hand, the use of web beacons is very common, (only Austria, India and Serbia have lower than 50%).

**Table 1: Percentage of websites using forms**

| COUNTRY | FORMS | FORMS USING GET |
|---|---|---|
| Australia | 60% | 53.3% |
| Austria | 100% | 70% |
| Canada | 89.3% | 53.6% |
| France | 100% | 100% |
| India | 100% | 70% |
| Israel | 80% | 55% |
| Italy | 100% | 80% |
| Japan | 100% | 100% |
| Pakistan | 100% | 70% |
| Serbia | 88% | 24% |
| Sweden | 100% | 40% |
| UK | 100% | 59.1% |
| USA | 90% | 55% |
| Total | 91% | 58.5% |

Table 2: Percentage of websites using cookies and web beacons

| COUNTRY | COOKIES | FIRST-PARTY COOKIES DENIED FOR DEFAULT INTERNET EXPLORER PRIVACY SETTINGS | THIRD-PARTY COOKIES | WEB BEACONS |
|---|---|---|---|---|
| Australia | 26.7% | 6.7% | 0% | 73.3% |
| Austria | 60% | 10% | 0% | 30% |
| Canada | 46.4% | 3.6% | 0% | 53.6% |
| France | 70% | 20% | 10% | 90% |
| India | 60% | 20% | 0% | 40% |
| Israel | 35% | 5% | 0% | 60% |
| Italy | 30% | 10% | 0% | 80% |
| Japan | 50% | 10% | 0% | 60% |
| Pakistan | 50% | 0% | 0% | 60% |
| Serbia | 36% | 0% | 0% | 48% |
| Sweden | 60% | 20% | 0% | 60% |
| UK | 45.5% | 4.5% | 0% | 68.2% |
| USA | 75% | 5% | 0% | 50% |
| Total | 48% | 7% | 0.5% | 58.5% |

Table 3: Percentage of third party links in websites

| COUNTRY | THIRD PARTY LINKS |
|---|---|
| Australia | 93.3% |
| Austria | 90% |
| Canada | 89.3% |
| France | 100% |
| India | 80% |
| Israel | 85% |
| Italy | 90% |
| Japan | 90% |
| Pakistan | 100% |
| Serbia | 96% |

| | |
|---|---|
| **Sweden** | **100%** |
| **UK** | **90.9%** |
| **USA** | **90%** |
| **Total** | **92%** |

**Table 4: Percentage of websites implementing the P3P policy**

| Country | P3P compact policy |
|---|---|
| **Australia** | **0%** |
| **Austria** | **0%** |
| **Canada** | **10.7%** |
| **France** | **10%** |
| **India** | **0%** |
| **Israel** | **0%** |
| **Italy** | **20%** |
| **Japan** | **0%** |
| **Pakistan** | **0%** |
| **Serbia** | **4%** |
| **Sweden** | **0%** |
| **UK** | **22.7%** |
| **USA** | **15%** |
| **Total** | **7.5%** |

As we can see from Table 3, the presence of the third-party links is very common in e-commerce websites worldwide.

Table 4 indicates a low rate of implementation of the P3P compact policy on e-commerce websites (maximally about 20% in Italy and the UK).

## *The Results of the Second Investigation*

There were 134, or 62.62% of websites with privacy policy from all processed websites (214), but if we exclude domestic websites this number increases to 77.24% (112 out of 145). Only 22 out of 69, or 31.88% of the domestic websites were with this policy.

Analyzing various banks' websites we can see that from 20 foreign banks 17 have privacy policy, and from 12 domestic only 2. We believe that every bank has to take care about clients' privacy.

It is interesting that several eminent domestic Internet providers with a large client population do not have a privacy policy. In addition, domestic on-line newspapers, TV and radio stations mostly do not have privacy policy. Several domestic on-line shopping companies, with substantial advertising in media, are without a privacy policy statement.

It is very notable that Verbatim promoted as "a major corporation that is highly regarded as a world leader in premium quality storage and imaging products" is in the same group.

We analyzed privacy policy statements in various websites, to see what it covers.

We were looking for all aspects of online privacy. The first five specify the data being tracked. These aspects are about data collecting, and they define who is collecting, what information is being collected, for what purpose, which information is being shared with others, and who they are. The next four are about the site's internal privacy policy. Can we change the way of using our data, can we define it, what about data retaining, and where can we find the privacy policy in a "human readable form"?

Some websites offer a shorter version of Privacy Policy, and propose user to read the full version. The complete Privacy Policy explains which information is collected, purpose of collecting, and how it is collected. Also, it presents one's ability to edit and delete your account of information and preferences.

To protect children's privacy and safety online many sites include in their privacy policy a special note for parents, according to The Children's Online Privacy Protection Act, (COPPA) effective April 21, 2000. The Children's Online Privacy Protection Act of 1998 is a United States federal law. It applies to websites and online services that are directed to children younger than 13, or have knowledge that they are providing information online. For example, Philips has a recommendation for parents to supervise the online activities of their children under thirteen, and BitTorrent notices that it does not collect personal information from children under 13.

About personal data sharing many sites offer mostly general information without stating clearly what is shared and with whom. Phillips cites that personal information may be transferred to other Phillips companies and third parties outside Phillips. Motorola shares "with reputable third-party advertising company" website usage information about visitors collected through gifs (the use of pixel tags). Nokia shares personal visitor data with "subcontractors" who can provide services to them. It is similar with Apple, but it is added that it may be required by law or litigation to disclose visitors' personal information, and that those may be disclosed if that is necessary for issues of public importance. On the NBA.com website are namely quoted members of the NBA family and also is referred to companies (Amazon.com, Getty Images) engaged to perform services in connection with the management and operation of the NBA family members. Most websites recommend users to review the posted privacy of third parties for more information.

## Suggestions for Website Privacy Improvement

In supporting online privacy participate:

▪ **Users.** When surfing the Web users should utilize the tips mentioned in section *Hints for users to help protect their own privacy online* in order to protect their own personal data.

▪ **Companies.** A minimum effort a company can do in order to support online privacy of their customers is to place a privacy policy on the company's website. Writing such a statement is not difficult any more, since there are several services on the Web doing it for free. For example, ("The DMA's Privacy Policy Generator," 2007) offer website owners a form with several questions about user tracking and user data storing. After submitting the form, the website owner gets a html page with an automatically created privacy policy. The appropriate web page is ready to be placed on the website!

A more complicated matter for the web designer is to write a p3p policy. Maybe that is the reason the p3p policy is so rarely found on the Web. But fortunately, a p3p policy can be written within a few minutes by using appropriate online services (P3P editor: http://p3pedit.com/, P3Pwriter Real Time Privacy Policy Editor: http://www.p3pwriter.com/) for a low fee of approximately $40.

- **Educational institutions.** Nowadays the Internet becomes a powerful support in education, and all students have to be informed about protecting their privacy when on the Web. Therefore we have involved this content in the syllabus of our introductory IT course.

Web designers have to be aware of the importance of the users' privacy. Therefore web users' privacy issues have to be included in their education. In that way they can understand that web design is not just a technique for skills' promotion, but a serious job with many more responsibilities. They have to pay attention to many issues, and particularly to the security and protecting of user's rights and privacy.

Our study program Web Design includes subjects containing both technique and artistic aspects of creating websites. Also we have included in the syllabus a subject that involves teaching usability, accessibility, privacy etc. As said in Krunic et al. (2006) students have a low prior knowledge about the importance of those issues. Web designers should learn how to write a privacy policy and acquire knowledge about P3P.

## Conclusion

Nowadays, with the high growth of the Internet practice, everyone has to recognize opportunities, rights, and duties of the Internet use. Websites offer great possibilities for companies in their businesses and for users utilizing various online services. Both sides have soon become familiar with the Internet advantages.

For the users it is very important to be well informed about their rights, especially the protection of their privacy. On the other side, the companies have to execute their duties to avoid unsafe actions that jeopardize the user's privacy. Although many companies involve standards in their websites for this purpose, in many cases it is insufficient. The visitors are worried about misusing their personal data, and more efforts should be put in getting their confidence.

Also, it is very important for IT education institutions to educate users on how to protect their confidential data when surfing the Web, and also to educate the future web designers to respect the user's privacy. In addition, users have to be informed how companies track their information, since they sometimes panic without reason. As it can be seen in our investigation, users do not have to be afraid from first party cookies, since they are mainly used for their benefit, although the cookies are notorious for the users fear them most.

On the other hand, users should be afraid from web beacons and third party content. However, they should mostly take care about easy giving of their personal data to websites which offer suspicious transactions, like low price purchases and alike.

## References

ABC's of Online Privacy. (2003). Privacy Call for Action. Retrieved from www.callforaction.org

Cookies – What they are and how they are used. (2005). Retrieved from http://www.spywareinfo.com/articles/cookies

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 Communication Sector, Official Journal of the European Union. (2002). Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML

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). Retrieved from http://www.cdt.org/privacy/eudirective/EU_Directive_html

The DMA's privacy policy generator. (2007). Retrieved from http://www.the-dma.org/privacy/creating.shtml

DoubleClick. (2007). Retrieved from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/DoubleClick

Internet scams fraud trends, January-December 2005. (2005). Internet Fraud Watch.

Jamsa, K., King, K., & Anderson, A. (2002). *HTML & Web design tips & techniques*. The McGraw-Hill Companies

Knowledge Leader. (2006). Retrieved from www.knowledgeleader.com/iafreewebsite.nsf/content

Krunic, T. (2006). *On-line shopping user privacy support in Serbia and Montenegro*, The 6-th International Conference on Electronic Commerce and Electronic Business, Palic (2006).

Krunic, T., Ruzic-Dimitrijevic Lj, Petrovic, B., Farkas, R. (2006). Web Design Curriculum and Syllabus Based on Web Design Practice and Students' Prior Knowledge, Journal of Information Technology Education, Volume 5. Available at http://jite.org/documents/Vol5/v5p317-335Krunic153.pdf

The National Law about Advertising (Nacrt zakona o oglasavanju). (2005). Retrieved from http://www.anem.org.yu/download/nacrt_zakona_o_oglasavanju.doc [Available only in Serbian].

P3P & Privacy on the Web FAQ. (2002). Retrieved from http://www.w3.org/P3P/p3pfaq

Platform for Privacy Preferences (P3P) Project. (2007). Retrieved from http://www.w3.org/P3P/

Powell, T. A. (2000). *Web design: The complete reference.* McGraw-Hill.

Privacy matters. (2001). *Journal Micro* [in Serbian: Pitanja privatnosti, arhiva casopisa Mikro] Retrieved from http://www.micro.co.yu/ser/vesti/arhiva?php=2001&mesec=5

Privacy tips. (2003). Retrieved from *BBBOnLine* (a subsidiary of the Council of Better Business Bureaus) http://www.bbbonline.org/UnderstandingPrivacy/toolbox/tips.asp

Rules and Tools for Protecting Personal Privacy Online. (2003). Retrieved from the Online privacy alliance http://www.privacyalliance.org/resources/rulesntools.shtml

Simovic, V. (2006). Credit card fraud in E-business. *The 6th International Conference on Electronic Commerce and Electronic Business,* Palic (2006).

*Trends and Attitudes in Information Security.* (2006). RSA security e-book retrieved from www.rsasecurity.com

*What is a web beacon?*, http://www.webopedia.com/term/w/web_beacon.html, (2005)

*Why implement P3P?* (2005). The P3P implementation guide. Retrieved from http://p3ptoolbox.org/guide/

# Appendix

## *A list of Websites Checked by WEBXACT*

**Australia**

http://www.sunshinecomputers.com.au

http://www.about-australia.com

http://www.aussiebest.com

http:// www.aussie-shopping.com

http:// www.perfume.com.au

http://www.latestbuy.com.au

http://www.haabaa.com

http:// www.freestylemedia.com.au

http:// www.abc.com.au

http:// www.aboriginalaustralia.com

http://www.shopsafe.com.au

http://www.shoptheweb.com.au

http://www.coastshop.com.au

http://www.ozeworld.com
http://www.woolworths.com.au

**Austria**

www.eplanetshopping.com/newfront/main.asp
www.vienna.at
www.timeout.com/travel/vienna
https://ssl22.inode.at/shop.manova.at/catalog/
www.sony.com
www.freestylemedia.com.au/download.asp
http://shop.abc.net.au/help/viddvdinfo.shtm
www.ncbuy.com/travel/health/report_country.html?code=au
www.dongabriel.net
www.vienna-hotels.inn26.com

**Canada**

www.800florals.com
dmoz.org
www.glacombe.com
www.infoedmonton.ca
www.canadashoppingcanadian.com
www.clickz.com
www.ducks.ca
www.canuckabroad.com
www.cndcountrygifts.com
www.canadacomputers.com
www.greatcanadianshopping.com
www.buyitcanada.com
www.walmart.com
www.costco.com
www.quixtar.com
http://www.nature.ca/prodserv/cat/main_e.cfm
http://www.readersdigest.ca/store_home.html
http://www.pitneybowes.ca/support/faq_onlineshopping.asp
http://www.searchon.ca/search/search.pl?Terms=shopping
http://www.digitalgravel.com/Testi.cfm
http://www.insure.com/
http://www.terencanada.com/
http://canada.aol.com/press/press_10_25_05.adp
http://www.eplanetshopping.com/ca/
http://www.qualityfoods.com/
www.feelbest.com
www.glacombe.com
www.infoedmonton.com

**France**

fr.shopping.com
www.ebay.fr
www.alapage.com
fashion.about.com
www.wanadoo.fr
www.lingerie-direct.com
www.voila.fr
www.1855.com
www.chateaunet.com
www.allo-webmaster.com

**Germany**

www.bellnet.de
www.lycos.de
www.de.dir.yahoo.com
www.web.de
www.yipi.de
www.chemie.de
www.flix.de
www.zdnet.de
www.glist.com
www.sharelook.de

**India**

http://shop.indiainfo.com
shopping.expomarkets.com
http://shopatchitralekha.tolshop.com/
http://www.ebay.in
http://www.captainartsandcrafts.com/enquiry.htm
http: //www.indiangiftsportal.com/
http://www.fabmall.com/
http://sify.com/shopping/
https://www.sirindia.com/index.asp
http://shop.nirula.com/

**Israel**

www.iguide.co.il
www.myisraelsource.com
www.internetstorelist.com
shop.katif.net
www.israelaustin.com
israel.zeezo.com
dmoz.org
www.allhlwines.com
www.livnot.com
www.israzon.com
www.israel-shops.com/
www.israelseed.com
judaism.about.com
1800sunstar.com
www.machers.com
www.jcolstore.com

abcnews.go.com
www.igourmet.com
www.cjp.org
www.flowers.co.il

### Italy

http://www.maptown.com/deskglobes.html
http://www.bigsoccershop.com
http://www.united-states-flag.com/italy3x5p.html
http://www.bizrate.com/
http://bluespirit.vstore.ca/
http://news.earthweb.com/
http://www.italiamia.com/shopping.html
http://search.modaitalia.net/
http://www.elib.org/
http://www.ebay.it/

### Japan

www.outdoorjapan.com/marketplace/
www.planetliquor.com/japan/
www.yourdictionary.com
www.tnt-pc.com
www.cathaypacific.com
www.addall.com
www.sonore.com
www.japanvisitor.com/jc/links/japan-shopping-links.html
toy.avantzone.com
www.gridskipper.com

### Pakistan

www.worldofinternetcafes.de/Asia/Pakistan/fpcci.com.pk/chambers.asp
www.nowarzone.org/journal.aspx?ID=530
www.pocketmail.com/journal/
www.adbrite.com/mb/dir.php?page=4&a=20002.1.44012
www.adbrite.com/mb/dir.php?a=44012.1.20002&page=4
www.tradekey.com/ks-PP-jumbo-bag/
hughw36.blogspot.com/2003_12_28_hughw36_archive.html
www.askwebhosting.com/whc/2004/web_hosting/Manhattan/
www.sunnisisters.com/sunnisister/?comments_popup=758

### Serbia

http://www.yu-oglasi.com/racunari/messages/791.html
http://www.yu4you.com/
http://www.pcpress.co.yu/kupovina.asp
http://daliborpetkovic.tripod.com/
http://www.vidi.hr/top100/prijave/internet_p.html
http://www.myshop.co.yu/
http://www.robnakuca.com/mailom.htm
http://www.videofilmovi.com/
http://www.karaoke.co.yu/narudzba.html
http://www.2net.co.yu/shop/
www.yusearch.com/start/index/
www.zoopage.co.yu/
www3.ptt.yu/kategorije.php?section_1=3
www.list.co.yu/cms.php?a=Artikli&as=45&t=72
www.recepti.co.yu/recepti/sponzor.asp?IDsponzor
www.e-trgovina.co.yu/
www.pretraga.co.yu/direktorijumi/yuguide/index.php?k=4
www.kupovinaonline.co.yu/content/view/24/56/
www.pctv.co.yu/internet/etrgovina.htm
www.svezaskolu.co.yu/prezentacija/index.php
www.dafis.co.yu
www.011shop.co.yu
www.hi-fi.co.yu/index.php
http://www.net-yu.com/public/shop/products/listProducts.php?&lang=en
www.microgen.co.yu

### Sweden

www.nsd.se
hadelandlag.org
www.argus.nu
www.catahya.net
www.byggahus.se
www.darkdisc.com
eforum5.idg.se
www.alltforforaldrar.se
www.fuska.nu
zatzy.com

### United Kingdom

www.british-shopping.com
www.4ukshopping.co.uk
www.ishop.co.uk
www.marksandspencer.com
www.next.co.uk
www.shoppingtrolley.net
www.shopsafe.co.uk
www.ukoffer.com
www.uk-shoponline.co.uk
www.waitrose.com

http://www.kelkoo.co.uk/
http://www.tsoshop.co.uk/
http://www.play.com/
http://www.shopperuk.com/
http://www.argos.co.uk/static/Home.htm
www.gymuser.co.uk/shopping/shopping.htm
http://www.virginmega.co.uk/
http://www.ebay.co.uk/
http://www.phones4u.co.uk/
www.onevillage.org
http://www.picwines.co.uk/
http://www.ciao.co.uk/paid_surveys.html

**USA**

http://www.mysticalgift.com/xAuraSoma.aspx
http://www.usatf.org/store/
http://www.konicaminoltastore.com/
http://www.bella-usa.com/
http://www.ecost.com/ecost/ecsplash/default_new.asp
http://disneyshopping.go.com/
http://esprit-usa.com/Merchant2/merchant.mvc
http://www.cduniverse.com
http://www.ica-usa.org/Merchant2/merchant.mv?Screen=CTGY&Store_Code=ICA&Category_Code=courses
http://store.campfire-usa.org/FAQ/Index.asp?IdS=000A1F-FDC5380&Reference=GiftCertificates&~=
http://www.compusa.com/
http://www.sony.com/
http://us.penguingroup.com/
http://www.fedstats.gov/
http://www.ikea.com/ms/en_US/
http://greenvilleonline.com/apps/pbcs.dll/frontpage
http://www.nashbar.com/index.cfm
http://shopping.localstreets.com/xml/en/United_States/cate_840___0.html
http://store.palm.com/home/index.jsp
http://www.usatoday.com/tech/news/2005-11-27-cyber-monday_x.htm

## Biographies

**Tanja Krunić** is a lecturer at the Advanced Technical School, Novi Sad, Serbia. She teaches courses in web design and Internet languages and tools. She holds a MS in mathematics and is currently working towards her PhD in Numerical Analysis from the Faculty of Mathematics and Natural Sciences, Novi Sad. Her research interests include important issues like usability, accessibility, privacy, and security on the World Wide Web.

**Ljiljana Ružić-Dimitrijević** is a professor at the Higher Education Technical School of Professional Studies, Novi Sad, Serbia. She teaches courses in Computers, Introduction to web design, and Development of the Internet. She got her MSc degree in mathematics at the Center of Multidisciplinary Studies, Belgrade in 1991. Her field of expertise is computer graphics and web design. She is pro-dean in charge of tuition.