In order to avoid the potential for disputes between US companies and the EU, the US Department of Commerce and the European Commission created the Safe Harbor privacy framework, whereby US companies can verify that they will treat data collected from within the EU zone according to the standards outlined in the EU Directive. US companies can certify that they conform to the principles of the Directive, though the process is entirely voluntary, and can be undertaken either by joining a self-regulatory program (we look at one in the next section), or by developing their own program that conforms to the Safe Harbor framework.

The advantages to an organization conforming to the Safe Harbor framework are chiefly that they will accordingly be able to continue to do business with EU citizens and companies without interruption, and that any claims brought by EU citizens against US companies will, in most cases, be heard in the US. More information on the Safe Harbor framework can be found at the US Department of Commerce web site: *http://www.export.gov/safeharbor/*.

COPPA

The other significant piece of US legislation that we need to cover is the Children's Online Privacy Protection Act, known as COPPA. This Act sets out the legal framework for the collection of "personal information" from children under the age of 13. It applies to all web sites or "online services" that are aimed at children under 13 and that gather personal information from their users, and also to general web sites that have "actual knowledge" that they are collecting personal information from children.

"The clear aim of this legislation is to safeguard the privacy of young children who may not be aware of the potential dangers of disclosing personal information over the Internet."

The clear aim of this legislation is to safeguard the privacy of young children who may not be aware of the potential dangers of disclosing personal information over the Internet. The Act covers information that individually identifies the child, such as name, address, e-mail, telephone, or anything that would allow someone to contact the individual. It also includes information such as hobbies and, importantly, information gathered by the use of cookies or other tracking devices "when they are tied to individually identifiable information" – that is, the cross-referencing of cookie data, such as pages visited by an individual, with that individual's contact information.

The Act places various constraints on the web sites to which it applies, the principal one being that the site must publish a clear and unambiguous privacy policy, and this should have a "prominent" link on both the home page of the site and any other page where personal information is collected. The Act specifies that the policy should state:

- Who is collecting the data – including the name, address, and e-mail address of at least one contact, and the names of any other parties ("operators") involved with the collection of data on the site

Amazon/AlmondNet
Exhibit 1011
Page 31

- What data is collected and how – included the use of cookies if appropriate
- Specifically what this information will be used for (direct marketing, sending an opt-in newsletter, etc.)
- Whether the information will be distributed to third parties, and if so for what purpose and with what safeguards. Also, parents must have the right to opt out of this third-party distribution of their child's information
- That no unnecessary information may be collected for the purposes of participation in the activities of the web site
- The parent's right to view, and if necessary remove, their child's personal information, and remove consent for further collection, as well as clear instructions as to how to carry this out

There are also a number of suitable definitions, clarifications, and exceptions to these rules, for example detailing what can be collected without the explicit consent of a parent. Nevertheless, the basic thrust of the Act is clear: when dealing with young children, the responsibilities of the web site for privacy and data protection are heightened, and explicit care must be taken to outline what is collected, why, and how the child or parent can intervene in the process.

Other Organizations

As the whole landscape of privacy, data protection, and legislation is complicated enough for web professionals, it is especially important to engender trust in the mind of the user. To this end, there are various organizations whose aim is to increase this sense of trust, and work with partner web sites to bring it about. Two such groups are BBBOnline *(http://www.bbbonline.org/)*, run by the Council of Better Business Bureaus, and TRUSTe (*http://www.truste.org/*), an independent non-profit organization founded by the Electronic Frontier Foundation (EFF) and the CommerceNet Consortium. Both of these organizations have similar objectives and programs.

> *"users have the right to know what is being collected about them"*

The general reason for the existence of organizations like BBBOnline and TRUSTe is to generate a greater sense of trust in Internet users, and the explicit policies that they advocate are broadly in line with the principles of the legislation that we have examined above. In short, users have the right to know what is being collected about them, what will be done with this information, including whether it will be further distributed, and the right to opt out of certain uses of the data, for example for direct marketing campaigns. The key to this is transparency: a privacy policy that states exactly what is being done, and what the user can do about it.

Amazon/AlmondNet
Exhibit 1011
Page 32

With this objective of establishing clear and authoritative privacy policies, both of these organizations offer "Seal Programs", effectively underwriting the privacy policies of affiliated sites, and offering their "Seal" to indicate this. Whilst the details of how to join these programs vary, the basic principle is that the web site submits its privacy policy and data collection practices for review by the program. If the site meets the requirements of the program, both in terms of the policy itself and its general data practices, then it can be awarded the Seal (there is a fee for this service).

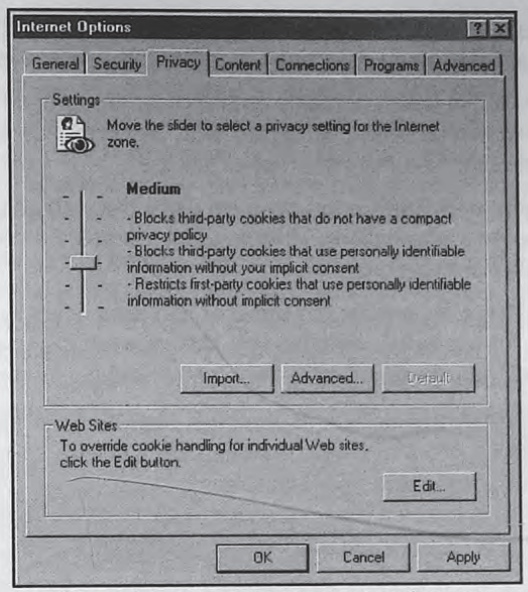
These programs also undertake to arbitrate in the case of any visitor entering into a dispute with the web site in question, and the site can be suspended or expelled from the program if it fails to live up to its promises, a facility designed to increase the level of trust and confidence in the web site's users. In addition to the main Privacy Seal Program, BBBOnline and TRUSTe also offer other programs, validating such things as children's privacy, and Safe Harbor compliance.

The Platform for Privacy Preferences Project (P3P)

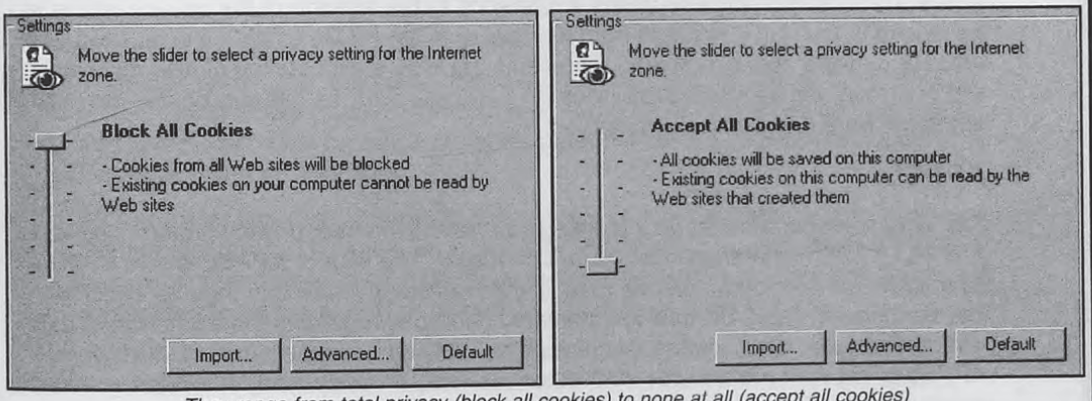
A further attempt to clarify and simplify privacy for both web site operators and users has been made by the W3C in the form of the Platform for Privacy Preferences Project, commonly known as P3P. In essence, this is a project to standardize the information contained within privacy policies, and to encapsulate that information in a **machine-readable form**. The idea behind this is that if privacy policies can be made available in such a way as to be understandable to the user's computer, then this removes from the user the task of reading and interpreting the written version, effectively automating the task, once the initial preferences have been set. The idea is that this would make it far more likely that web sites' policies will be reviewed each time data is transferred.

This is an emerging standard for the construction of privacy policies, and with the credible backing of the W3C, so it is worth examining in a little more detail. Let's now take a brief look at how P3P works, what the web site operators and users need to do to use it, and discuss what effect this will, and will not, have on online privacy. There is some built-in support for P3P in Internet Explorer 6, Netscape 7, and as an additional feature for Mozilla (see *http://www.mozilla.org/projects/p3p/* and *http://lxr.mozilla.org/mozilla/source/extensions/p3p/*). Internet Explorer 6 now has a *Privacy* tab on the *Internet Options* dialog, allowing a simple selection of privacy preferences:

Amazon/AlmondNet
Exhibit 1011
Page 33



IE6 now lets you select your privacy preferences



They range from total privacy (block all cookies) to none at all (accept all cookies)

P3P is a protocol for computers to exchange detailed information about privacy policies, in effect a language for discussing privacy. Specifically it defines a way in which a normal "natural language" privacy policy can be translated into an XML format, which user agents – browsers in most cases – can access, and check against a pre-defined set of preferences. A typical sequence of events is as follows:

1 A web site operator establishes what their privacy policy is, and writes a natural language version of it for display on the site.

Amazon/AlmondNet
Exhibit 1011
Page 34

2 The operator then translates this into an XML file using the P3P standard. There are various tools being developed to make this process easier.

3 Another XML file which contains details of where to find the policy is then placed in a "well-known location", which the W3C recommends is `/w3c/p3p.xml`, where the `w3c` directory is under the root of the site.

4 A user agent with P3P preferences set visits the web site, locates the privacy description and automatically downloads it, parses the contents, and compares it with the user preferences.

5 Based on this comparison, the browser can automatically elect to exchange data (a cookie, for example), with the web site, or warn the user that the site does not meet the standards specified in the preferences file in some way.

IBM is developing a P3P Editing tool, currently in beta, to ease the process of translating a written privacy policy into a machine-readable format (XML file). At the time of writing, this tool is free to download and use, and is available at: *http://www.alphaworks.ibm.com/tech/p3peditor*. A list of other implementations is available from the W3C web site: *http://www.w3.org/P3P/implementations*.

The location details do not necessarily have to be placed on the web site as detailed above. The specification also allows a reference to the location of the privacy details to be placed in the HTTP headers from the site, or in the HTML using a `<link>` tag. The process outlined above, however, represents the W3C's expectation of how most web site operators will deploy the reference in `/w3c/p3p.xml`, as this is probably the most straightforward and transparent method.

APPEL

The W3C are also working on a language for describing user privacy preferences, called APPEL (A P3P Preferences Exchange Language). The idea of **APPEL** is that it will be used to create sets of preference rules (called rulesets), which can then be imported into the browser (say) for making automated decisions regarding the exchange of data with web sites or other remote machines. The W3C do not expect individuals to learn APPEL to set their preferences, but rather use tools or ready-made rulesets to make the process easier. Existing rulesets, most likely created by a third party, can be imported into a browser, and indeed exchanged between different browsers operated by the user.

So now it seems we have at least an emerging standard for describing our privacy policy and automating the process of checking it. What is this designed to achieve? The wider adoption and implementation of P3P should:

Amazon/AlmondNet
Exhibit 1011
Page 35

- Make privacy policies more accountable. If browsers are automatically checking the details of a web site's policy, and acting accordingly on the preset user preferences, this will not only force sites to declare their policies unambiguously, but also ensure that the policies themselves are in line with their users' expectations. The principle is that privacy will become a more transparent process, meaning that users will be able to see clearly where they stand, and make informed decisions as a result.
- Enable users to have more control over their privacy and use of their personal information. It is unlikely that users currently check privacy policies in any detail (if at all) when visiting a site or exchanging data, largely due to the time needed to locate the policy and check it for potential problems. Automating the system, so long as the preferences-setting part of the process is clear, should increase awareness and control.

It is important to make clear, though, what P3P cannot do:

- It has no power to ensure that web sites actually abide by the privacy policy that they publish. There is nothing in the W3C specification that prevents a site from using P3P in an attempt to deceive their visitors. It could be argued that, as the system is automated, this may increase the potential for abuse, because users will begin to "trust" the browser to tell them when something is wrong. In fact, they should be trusting the web site, not P3P. In this respect, nothing has changed, as a site has always had the power to publish a misleading, or indeed false, privacy policy. This is where organizations such as TRUSTe or BBBOnline can be useful, and in fact P3P does contain a `DISPUTE` element in which dispute-resolution information can be described.
- P3P is not designed to supersede or replace statutory regulations, but rather complement them. The intention is that P3P will assist in the assertion of legal frameworks, and encourage a better understanding and conformity with them, but it cannot enforce them. Proper regulation and P3P go hand in hand.
- There is no provision for encryption or the security of data within the P3P specification. P3P does not replace the need for encryption and secure data exchange, but again complements it, by allowing the user to get a clear picture of what is being done, and to respond accordingly.

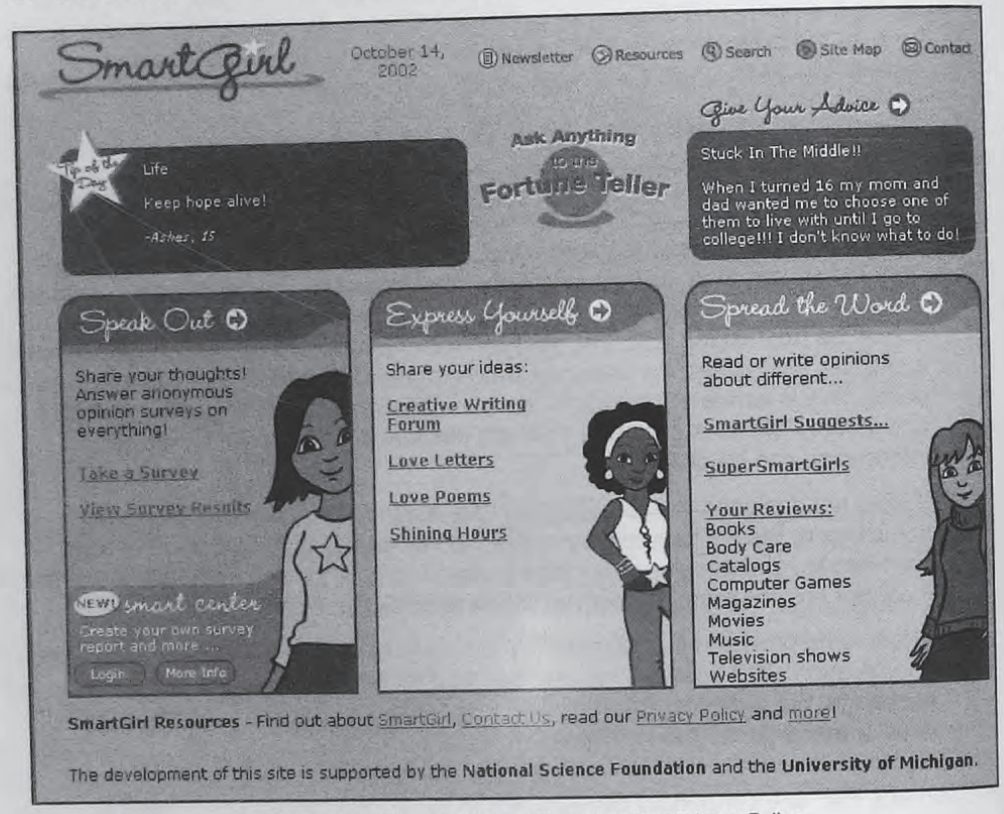
In summary, P3P is an important development in the privacy landscape. It has the authority of the W3C behind it, and has the support of many leading industry groups and companies. The adoption of P3P at the moment is somewhat nascent, but as newer browsers include elements of the specification in their upgrades, more users will become aware and able to take advantage of its preference checking process. In this respect, it will place the onus on web site operators – owners, managers, and developers – to create a clear privacy policy and implement it in P3P.

Amazon/AlmondNet
Exhibit 1011
Page 36

Case Studies: Real Life Privacy

We have so far covered something of the theory and the rules concerning online privacy, but the picture would not be complete without taking a look at how real sites are reacting to the situation. In this section we will discuss three different sites: *The Onion*, The New York Times, and *SmartGirl*. We will look at each site in turn, examining what it needs to do to maintain its business, what analysis is done, and how it explains this in its privacy policy. The information presented here is taken from interviews conducted with the help of the sites in question.

SmartGirl: www.SmartGirl.org



The front page of SmartGirl.org, with easy to find Privacy Policy

SmartGirl.org is a web site written for and by girls, many under 13 years of age, and therefore has to comply with COPPA. It is worth looking at how their exemplary privacy statement details what the site does and does not record, and the measures in place both to ensure compliance with the law, and create a safe and interesting place for girls to participate.

Amazon/AlmondNet
Exhibit 1011
Page 37

The policy begins with a statement of the site's purpose:

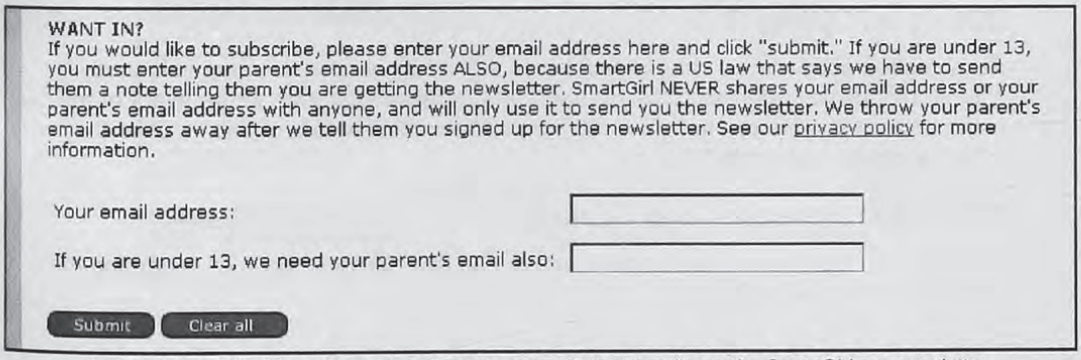
> This site is owned by the University of Michigan and is operated by the Institute for Research on Women and Gender. Our mission is to create a place on the Internet where girls can feel free and safe to express their opinions and views on everything from the latest movies and the hottest fashion trends to everyday issues like school, relationships and navigating adolescence. Girls visiting the site can fill out reviews on different products (such as books, movies and CDs), take anonymous surveys, play games, or submit love poems, love letters, and other content to be posted on the site. Girls who become members can participate in the SmartCenter.

It ends by disclosing the name and address of the site's operators, with both postal and e-mail addresses for contact in the event of any queries. In between, there is a very explicit description of SmartGirl's privacy procedures.

Personal Information

This is defined as any information that can personally identify an individual, such as an e-mail address. The policy states that no visitor to the site is required to disclose such information for the purposes of participating in the site, and any e-mail address provided is done so entirely voluntarily. Specifically, *SmartGirl.org* will never post, publish, rent, sell, or intentionally distribute personally identifiable information. All work submitted, or survey completed, is anonymous – users can include an e-mail address for the purposes of receiving notification as to whether their work will be published, but once used this e-mail address is no longer linked to the individual user.

If the user is under 13 years of age, then their parent's consent is also required for their submission of an e-mail address, for example to join the newsletter, or to receive notification if they have submitted work. This is requested at the same time, and a message is sent to the parent, which is then used to notify the parent that the child's e-mail address has been received, and give them the opportunity to remove it.



A parental e-mail address is required for girls under 13 to subscribe to the SmartGirl.org newsletter.

Amazon/AlmondNet
Exhibit 1011
Page 38

Parents can review their child's postings to the site, and change or delete their child's e-mail address or membership at any time. The privacy statement outlines the simple procedure for doing this.

User Tracking and Cookies

SmartGirl.org uses cookies for the following purposes:

- To track – anonymously – the traffic patterns on the site.
- To eliminate duplicate survey submissions.
- To allow members access to members-only content.

Crucially, cookies used for one purpose are not linked to cookies used for another purpose. For example, separate cookies are used for verifying survey submissions and traffic pattern analysis, and the two cookies are not identifiable as belonging to the same user. It is not possible to identify an individual user from the cookies stored on their computer. Other information, supplied by the web hosting company, is equally anonymous, and, similarly, released to third parties (such as advertisers) in aggregate form only. This information includes:

- Browser type and operating system (User-Agent)
- Sites referring users to *SmartGirl.org*
- IP address and Internet domains from which users are accessing the site
- Dates and times of distribution of traffic to the site
- Average length of stay on the site
- Pages visited

Opting In, Opting Out

As is implied above, the e-mail newsletter is strictly an opt-in list. Users voluntarily submit their e-mail address to be included on the newsletter and, in the event of the user being under 13 years of age, *SmartGirl.org* informs their parent of this, in case they wish to remove their child from the list.

Additional Measures and Security

In addition to the procedures detailed above, the site has strict policies regarding the security of the data collected:

Amazon/AlmondNet
Exhibit 1011
Page 39

Our Users' privacy and any personal information we may have about them are kept as secure as we are able, although like every other business entity, we cannot guarantee that this information will not be stolen. Passwords to access data at *SmartGirl* are only given to those trained to handle them safely. All *SmartGirl* staff members have signed confidentiality agreements that legally obligate them not to release e-mail addresses or any other information about visitors.

No personal information submitted by users is used for any purpose other than the stated reason for collection: e-mail addresses collected for the newsletter are used only to send the newsletter, and not for targeted mailings, for example. Furthermore, no personally identifiable information is ever distributed outside of the Institute for Research on Women and Gender Studies.

> *"e-mail addresses collected for the newsletter are used only to send the newsletter, and not for targeted mailings"*

The Onion: www.theonion.com



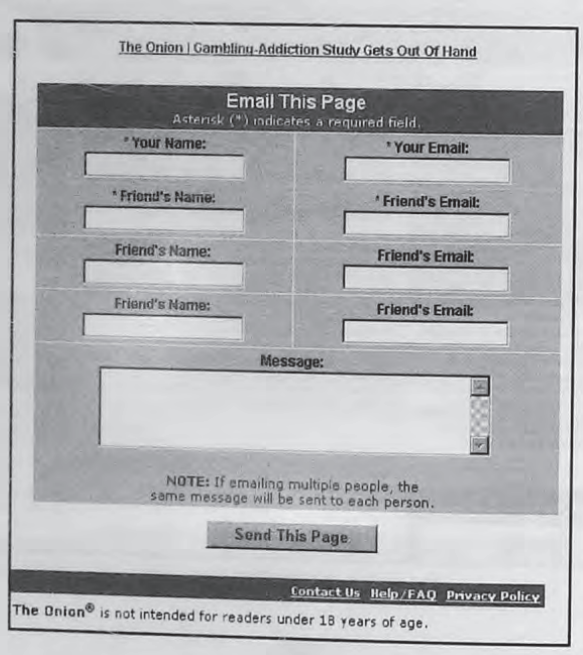
The well-known satirical news site.

Amazon/AlmondNet
Exhibit 1011
Page 40

The *Onion* is in the publishing business, which means that it makes its money by selling the print edition of the paper, and the advertising space therein. This is supplemented by its online business, which includes advertising sales, personals, and *The Onion store*, selling branded merchandising and other suitable wares. The online activity is important not only as a revenue stream in its own right, but also as a highly successful branding tool for the print publication. *The Onion* is aimed at an adult audience, with a notice declaring that it is not intended for readers under 18 years of age. Even though its content is irreverent and humorous, it takes online privacy very seriously.

Personal Information

The Onion collects and records personal information from customers, but only in order to fulfill orders that are made. This information includes the customer name, address, phone, e-mail (for order confirmation), and billing address if it is different from the shipping address. Credit card numbers are not stored by *The Onion*, but transferred to the card verification agent, *authorize.com*, who processes the order and confirms the result. If the transaction succeeded then the fulfillment details are forwarded to the fulfillment company for shipping. Users are able to register in order to speed up future interaction with the store, though this is entirely optional. Registration does, however, give the user the opportunity to review and amend any personal data that is stored about them on the site.



Amazon/AlmondNet
Exhibit 1011
Page 41

The only other collection of personal information on the site is the logging of e-mail addresses for the "E-mail this Story" feature. This is done as a security feature to protect *The Onion* from spam allegations. This information is not used in any other way.

Currently *The Onion* does not provide advertisers with demographic information gleaned from their campaigns on the site. Prior to a campaign, however, they are supplied with demographic data gathered from third-party sources (@plan, Nielsen) to help show potential clients the value of advertising with *The Onion.*

User Tracking and Cookies

Cookies are used on *The Onion* to maintain state during individual sessions. The information that this generates is then used to monitor visits to the site, though as the cookies are temporary – they expire at the end of the session – return visits by unique individuals are not tracked. An ad-tracking system – AdJuggler – is used to monitor general user responses to the ad campaigns on the site, in the form of ad impressions and click-throughs, but more detailed user interaction data is not recorded. The main purpose of the cookies used in advertising is to determine the frequency of the ads, and they use the cookie to control this for each unique visitor.

> *"The main purpose of the cookies used in advertising is to determine the frequency of the ads..."*

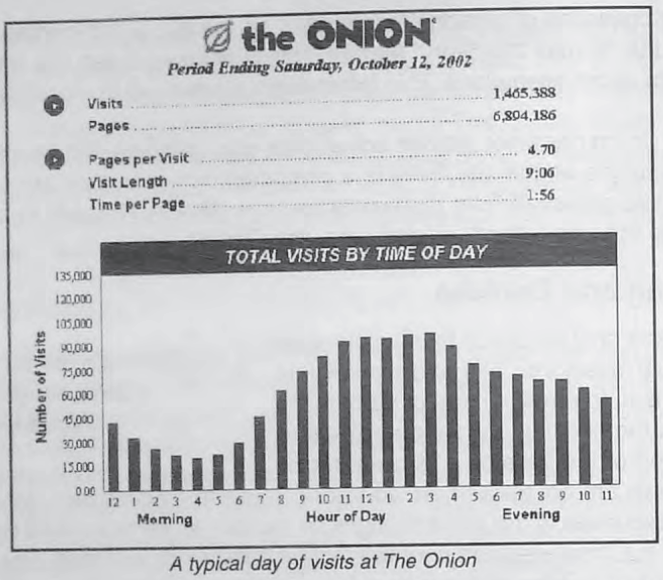
Cookies are also used for maintaining state as a customer moves through the shopping cart process. This cookie uses a unique anonymous user ID to keep each user distinct from others; the only data stored here is the expiration date and the name of the cookie, and no personal information is stored in these cookies. Each cookie is set using the ad system, or a piece of JavaScript embedded on each page.

> *"...no personal information is stored in these cookies"*

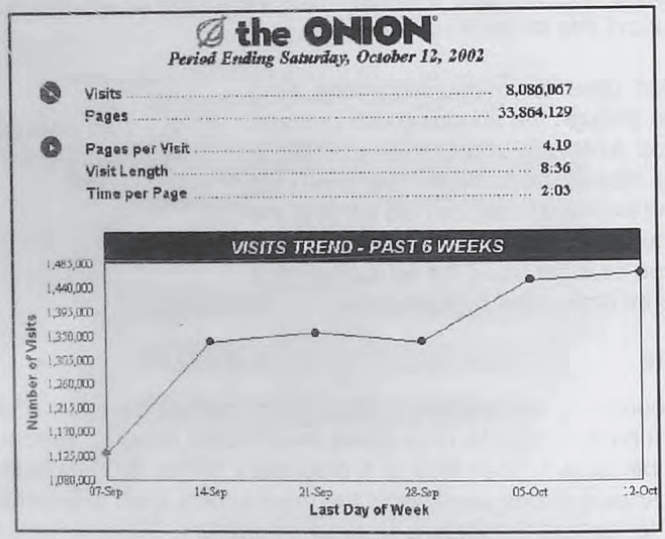
Data Analysis

The *Onion* outsources its log analysis to **I/Pro**, which gathers the information from the logs and sends it back in reports. I/Pro stores its extracted data in a database, but the final format can be `.xls` or `.csv` files, or a proprietary format for I/Pro Netline users. In addition to this, Analog is also used within the development team to generate more precise reports, for example, gathering browser version and OS data (from the User-Agent field). The I/Pro analysis is primarily to track page impressions, visits, and visiting organizations, resolved from the client IP address.

Amazon/AlmondNet
Exhibit 1011
Page 42



A typical day of visits at The Onion



The Onion is increasing its traffic

This log analysis is not formally audited by an outside organization (such as ABC Interactive), but I/Pro implements the standards as part of their service, for example by filtering out robot traffic and "false" impressions. They say: "We have a rigorous IP exclusions list that removes most known spiders and robots. This list is maintained and updated on a regular basis. With the new Netline release, we will also be excluding spiders and robots based on the User Agent in [*The Onion's*] logs."

Amazon/AlmondNet
Exhibit 1011
Page 43

Opting In, Opting Out

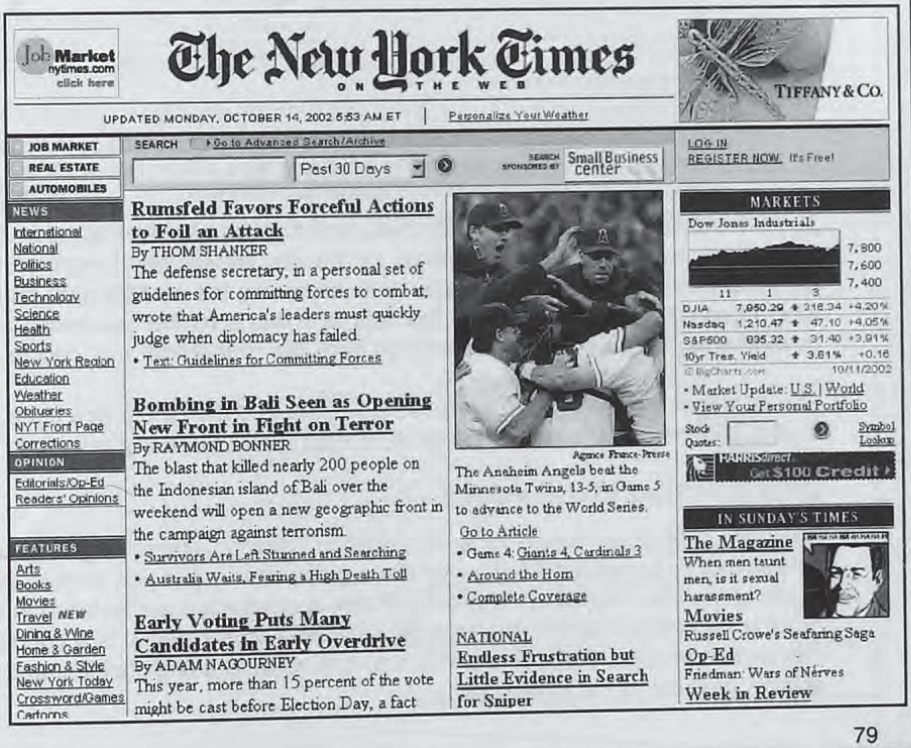
The Onion does not currently operate any lists that would require an opt-out, however if they were to operate such lists they would favor a "double opt-in" approach. On occasion, advertisers have used contest pages to entice consumers to sign up for e-mail lists. These are opt-in lists for the third party, and this fact is specifically spelled out on these pages with a link to the advertisers' privacy policy. Sometimes this information is collected by *The Onion*, and then delivered to the advertiser at the end of the campaign, but no e-mail from *The Onion* is ever sent to people who choose to sign up for these contests.

Double Opt-in

A single opt-in typically occurs when a user joins a mailing list by giving their e-mail address to the web site or list-manager. The drawback with this process is that the address could be submitted inadvertently by its owner or by a third party without the owner's consent. A double opt-in system does not add the e-mail address to the list on the first occasion, but rather triggers a message to the e-mail address itself, informing the owner that a request has been made to join the list, and soliciting a response. If no response is forthcoming, the e-mail address remains off the list. It is only added once the owner responds to the list's message, confirming that they wish to join. Members of the list have therefore had to "opt-in" twice before they are added.

The New York Times: www.nytimes.com

The well-established online news site.



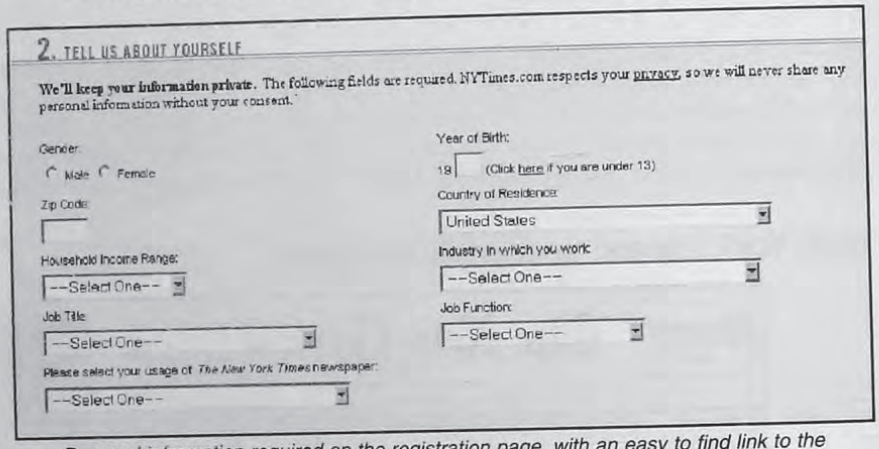
Amazon/AlmondNet
Exhibit 1011
Page 44

New York Times Digital is the name of the Internet division that includes *NYTimes.com*, *Boston.com*, and an archive distribution business.

New York Times Digital is in the "news and information business", its mission being to "enhance society by creating the premier quality network for everyone seeking the best news, information and interaction through digital media". The audience for *NYTimes.com* is global, with 85% outside of New York City, and 20% from outside the US.

Personal Information

NYTimes.com collects personal information about its registered users when they first register on the site, including details such as household income, Zip code (for US residents), and employment information. Notice that a statement referring the reader to the privacy policy is clearly visible on the following form:



Personal information required on the registration page, with an easy to find link to the NYTimes.com privacy statement

This information is only shared with third parties (such as advertisers) in an aggregated form, giving broad demographic trends for the site, except when required by law. The personal information is also available to its owner via the membership page on the site, where users can view and modify the data, and this is further password protected (users have to enter their password even if they have the "*remember me*" cookie set).

The demographic data is categorized by @Plan, and the categories used can be viewed on the *NYTimes.com's* online media kit, at *http://www.nytimes.com/adinfo*.

User Tracking and Cookies

NYTimes.com uses cookies for authentication, tracking usage, targeting and controlling ad serving, including identifying whether a given user is allowed access to "premium" areas of the site. The terms under which this is conducted are detailed in the site's privacy statement, which includes a detailed FAQ on cookies. It is a condition of the registration process that users consent to this tracking using cookies, and again, this is clearly spelt out in the privacy policy.

Amazon/AlmondNet
Exhibit 1011
Page 45

The privacy policy makes clear that their advertisers also use "clear GIFS", or "Web Beacons" – we've referred to these previously as "tags" – to monitor the ad-serving systems used on the site. The policy explains that this is happening, and outlines what is involved.

Data Analysis

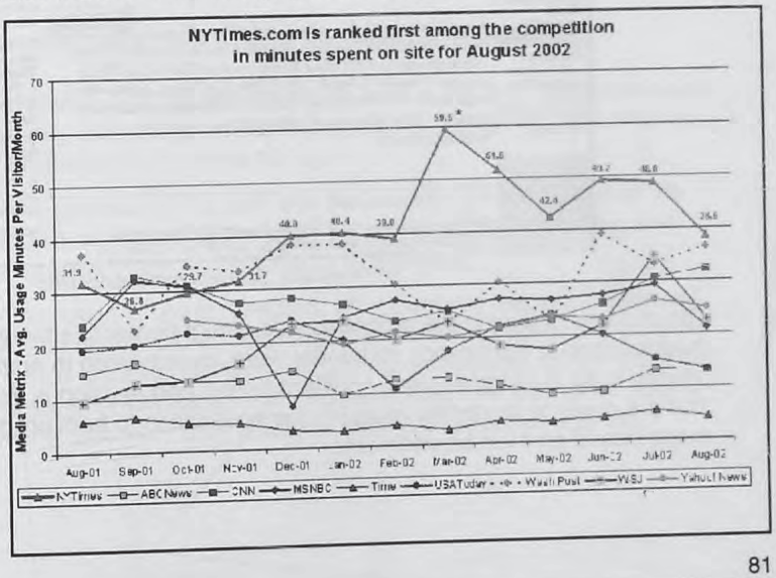
NYTimes.com uses an in-house log analysis system that parses the logs and reports the information, and also imports the data into an Oracle database. This allows them to conduct more specific queries on the data as the need arises. The output from the system can be in the form of HTML reports, which can be generated using a browser-based administration system, and Excel sheets and charts.

The system can track and report on:

- Usage patterns on the site
- Return visits for registered users
- Display of and response to advertising material
- Time spent by users on the site
- Visits referred from e-mails, including "*Today's Headlines*", which is sent to 3.3 million people every day
- International visitors (reported by comScore Networks)

Time spent on the site is considered to be a key indicator of visitor loyalty, and *NYTimes.com* currently leads the US news category in this respect.

NYTimes.com compared with other US news sites. Data from comScore Media Metrix



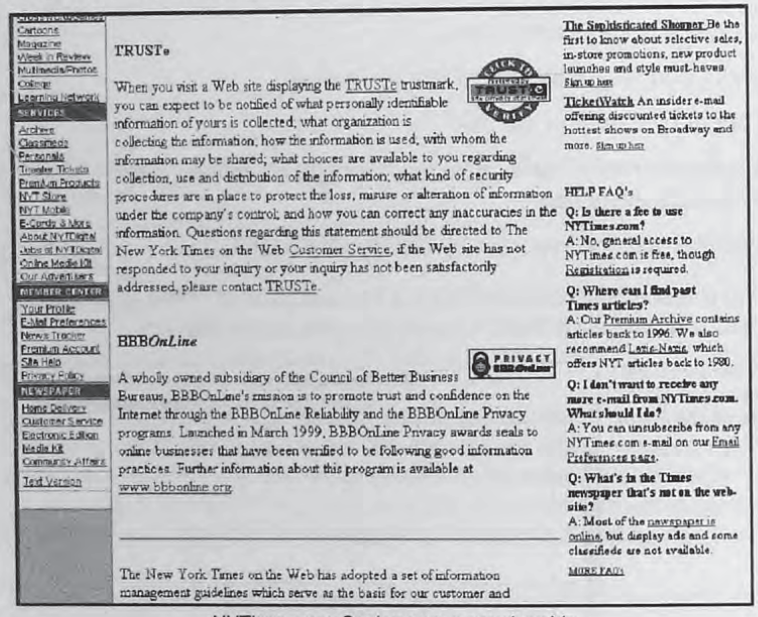
Amazon/AlmondNet
Exhibit 1011
Page 46

Opting In, Opting Out

All mailing lists on *NYTimes.com* are maintained on a strictly opt-in basis. When a new user registered, they are sent an e-mail to confirm this, and another two weeks later with additional information about the site. In the event of the user not returning to the site in a year, then they are sent one further e-mail. Membership of the mailing lists are available to the registered users via their membership page, where they can select or deselect checkboxes to join or leave each list.

Seal Programs

NYTimes.com is a member of two Seal programs, having joined TRUSTe in 1997, and BBBOnline soon afterwards. The reason for wanting to join these programs was that The New York Times is a trusted brand in print media, and it was important to continue this trust online. The Seal Programs were an excellent way of maintaining this, as they are recognized representing industry standards.


Cartoons
Magazine
Week in Review
Multimedia/Photos
College
Learning Network
SERVICES
Archive
Classifieds
Personals
Theater Tickets
Premium Products
NYT Store
NYT Mobile
E-Cards & Ideas
About NYTDigital
Jobs at NYTDigital
Online Media Kit
Our Advertisers
MEMBER CENTER
Your Profile
Email Preferences
News Tracker
Premium Account
Site Help
Privacy Policy
NEWSPAPER
Home Delivery
Customer Service
Electronic Edition
Media Kit
Community Affairs
Text Version

TRUSTe

When you visit a Web site displaying the TRUSTe trustmark, you can expect to be notified of what personally identifiable information of yours is collected, what organization is collecting the information, how the information is used, with whom the information may be shared; what choices are available to you regarding collection, use and distribution of the information; what kind of security procedures are in place to protect the loss, misuse or alteration of information under the company's control; and how you can correct any inaccuracies in the information. Questions regarding this statement should be directed to The New York Times on the Web Customer Service, if the Web site has not responded to your inquiry or your inquiry has not been satisfactorily addressed, please contact TRUSTe.

BBB*OnLine*

A wholly owned subsidiary of the Council of Better Business Bureaus, BBBOnLine's mission is to promote trust and confidence on the Internet through the BBBOnLine Reliability and the BBBOnLine Privacy programs. Launched in March 1999, BBBOnLine Privacy awards seals to online businesses that have been verified to be following good information practices. Further information about this program is available at www.bbbonline.org.

The New York Times on the Web has adopted a set of information management guidelines which serve as the basis for our customer and

The Sophisticated Shopper Be the first to know about selective sales, in-store promotions, new product launches and style must-haves. Sign up here

TicketWatch An insider e-mail offering discounted tickets to the hottest shows on Broadway and more. Sign up here

HELP FAQ's

Q: Is there a fee to use NYTimes.com?
A: No, general access to NYTimes.com is free, though Registration is required.

Q: Where can I find past Times articles?
A: Our Premium Archive contains articles back to 1996. We also recommend Lexis-Nexis, which offers NYT articles back to 1980.

Q: I don't want to receive any more e-mail from NYTimes.com. What should I do?
A: You can unsubscribe from any NYTimes.com e-mail on our Email Preferences page.

Q: What's in the Times newspaper that's not on the website?
A: Most of the newspaper is online, but display ads and some classifieds are not available.

MORE FAQ's

NYTimes.com Seal program membership

The process of joining the programs was straightforward, although some slight modifications to the privacy statement were implemented to ensure full compliance. As privacy is an evolving subject, constant review and revision is important. Any changes that are made to the policy must involve notification to both programs, and adjustments made based on their amendments.

Amazon/AlmondNet
Exhibit 1011
Page 47

Licenses from each program must be renewed annually, and approval requires the completion of a self-assessment report and questionnaire. Some time and resources are therefore required to manage the membership of the programs. *NYTimes.com* has a privacy committee with representatives from product development, marketing, PR, legal, and customer services departments, and this group meets regularly to discuss any privacy issues, industry developments, or policy changes. Online privacy is taken very seriously, and does require dedicated resources.

Summary

Privacy is increasingly important to the business of building and managing web sites as the general public (the users) become more aware of the issues and potential dangers to their privacy, and legislators begin to step in and rule on the subject. The overriding principle for the web site owner, however, is that good privacy is good business. By increasing the clarity of our privacy policies, we can increase the trust of those who use our sites, and so increase the potential for a more fruitful experience for everyone concerned, whether we are operating e-mail lists, publishing news services, or selling jam.

For this reason, it is advisable to have a privacy policy that is appropriate for our target audience. Owners of sites aimed at young children, for example, must exercise extreme care in their handling of users' information, but all sites that wish to develop a constructive relationship with their visitors (even those aimed at grown-ups) can benefit from taking privacy seriously. Many users will accept that certain information can legitimately be collected and used, to improve the site or service available, or to offer personalized content. Few web users will tolerate an incautious or dishonest attitude to their privacy rights, however, regardless of the legislation that may or may not apply.

Privacy policies should in most cases have at least the following attributes:

- It must be clearly available. This usually means at least a link from the home page of the site, and also any other page where information is being collected, such as an e-mail registration page, or an online survey.
- It must say who is the operator of the site, and particularly contact details in the event of a query or dispute regarding the site's privacy practices, including any accountability mechanisms (such as TRUSTe or BBBOnline).
- It must say what information is being collected, what purpose this information will serve, whether it will be distributed to other organizations or used for any purpose other than that for which it was submitted, and the consequences for the individual if they refuse to disclose certain information. For example, they will not be able to register for a "premium" service if they refuse to submit their postal address.

Amazon/AlmondNet
Exhibit 1011
Page 48

- It must say what measures the site takes to ensure the integrity and security of personal information that is stored, and the method for the individual to review, verify, and delete inaccurate or superfluous information.
- It must say which information the visitor has the right to opt out of, and which requires an opt-in (most commonly relevant to e-mail mailing lists, and the distribution of personal details to third parties or "carefully selected partners").
- It must say if cookies are used, and is so, give details. There is a lot of suspicion regarding the use of cookies, much of it unfounded, so the more explicit you can be the better. Explain what the cookie is, what it is used for, what it is NOT used for, and why it is in the user's interests to allow the cookie to be set.
- It must say where third parties are used, for example for the serving of ads on the site, or other partner programs. It must be explicit, and refer to the third parties' privacy policies if possible.

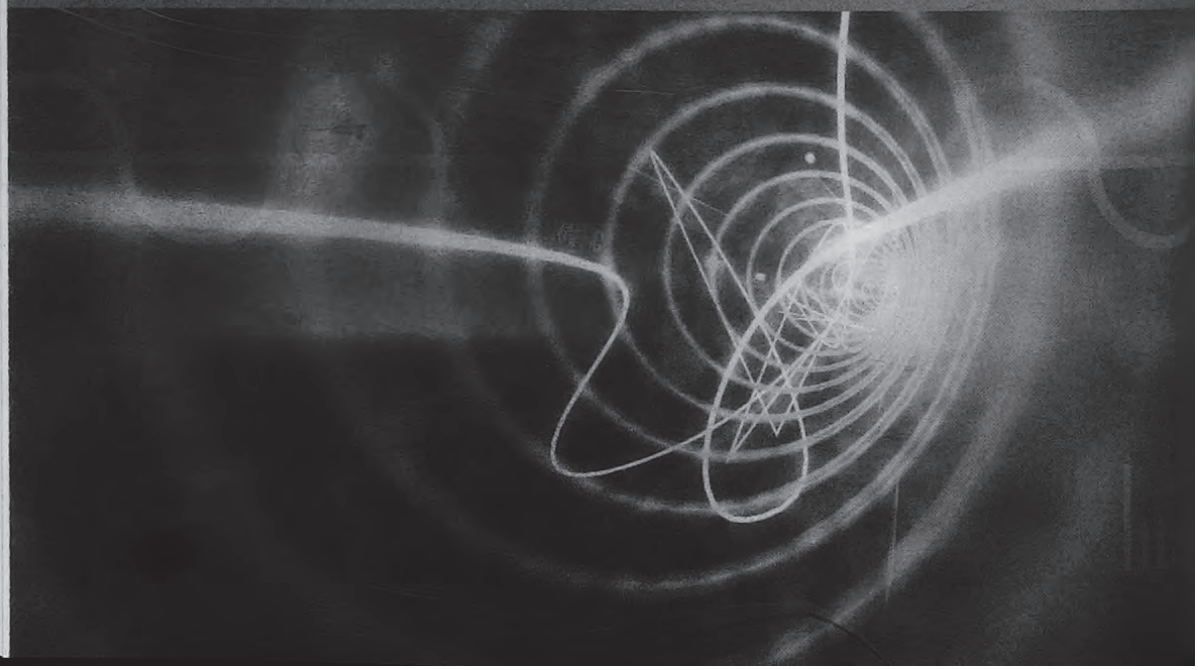
Emerging standards such as P3P are a useful tool for web site operators and users to talk to each other about privacy, but they are not a replacement for understanding the issues involved, and getting the policy right. Seal programs and similar self-regulatory schemes are another method available to us to increase trust and interaction, but again they are no replacement for understanding the needs and the concerns of our visitors, and ensuring that the requirements of the web site conform to them. Privacy is ultimately about openness.

Amazon/AlmondNet
Exhibit 1011
Page 49

4

- Rapid analysis informing editorial decisions
- Analyzing high demand
- Discovering how people use your site

Author: Peter Comber



Tools of the Trade

Practical Web Traffic Analysis

Standards, Privacy, Techniques, Results

Does your boss ask you for figures on how many visits the site gets – how long visitors stay – why they abort transactions? Do you lie awake worrying about referral logs, privacy policies, cookies and COPPA? What does the law say? What's the benchmark unit – hits? Unique visits? Pages served? AAARRGH!!

Writing Site Traffic Reports is one of the Ten Tedious Tasks of Web Professionals. But, with creativity and this book, Web traffic analysis can become a great way to get to know your users better, monitor which bits of the site are working, and which aren't.

This book includes all the code for a working Web Traffic Analysis System, and case-studies from The Onion, The New York Times, eBay ™, the BBC and SmartGirl.com (the latter looking at the legal and ethical implications of tracking young children's net behavior).

What you know:

Enough to have created a web site, be it client-side or server-side.

Optionally how to get server log files.

What you'll learn:

The techniques for gathering data on your users.

Standards and guidelines you should adhere to when interpreting your data.

What other sites are doing to ensure they respect the privacy of their users.

Insight into how three real sites use web traffic analysis.

glasshaus books: labor-saving devices for web professionals

http://www.glasshaus.com support@glasshaus.com

The three glasshaus web professional series:

Tools of the Trade:	Learning the tools web professionals use
Constructing:	Task focused – getting the web professional's job done
Insite:	Looking at successful sites that have achieved a balance of technology and design

Also Available



USA $29.99
CANADA $46.99

Sheiving Category: Web Development

glasshaus

or-saving devices for web professionals

apress™

ISBN 1-59059-208-5

52999

6 89253 15085 6

9 781590 592083