

EXHIBIT B

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

MIKE HARRIS and JEFF DUNSTAN,
individually and on behalf of a class of
similarly situated individuals

Plaintiff,

v.

COMSCORE, INC., a Delaware corporation

Defendant.

CASE NO. 1:11-cv-5807

Judge Holderman

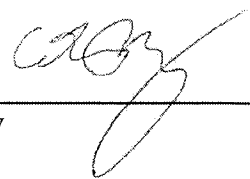
Magistrate Judge Kim

EXPERT WITNESS REPORT OF COLIN O'MALLEY

I have prepared this Expert Witness Report pursuant to Fed. R. Civ. P. 26(a)(2)(B) for the purpose of summarizing my forthcoming expert opinion testimony to be offered in the above-captioned case.

Dated: November 30, 2012

Colin O'Malley



Background:

Education:

- Stuyvesant High School, New York City
- Bachelor of Science, double major in Economics and Human & Organizational Development, Vanderbilt University

Experience:

I have been a product manager and an executive operating in the online privacy space for nine years. Over that time, I have designed best practice disclosure systems across a range of technologies and have engaged with stakeholders in industry, government, think tanks, and independent researchers around the world on this topic.

In 2003, I joined TRUSTe, the leading provider of privacy seals for websites on the internet¹ as a product manager. While at TRUSTe, I developed standards for consumer disclosure in the email marketing space for an accreditation service named Bonded Sender, which was developed in partnership with IronPort Systems. Bonded Sender was acquired by Return Path, a global leader in email services, and lives on today under a new brand as the leading whitelist program for commercial email senders that adhere to strong privacy practices.² I went on to lead the development of a seal program for email senders that could adhere to TRUSTe's strict privacy principles, called the Email Privacy Seal.³

In 2006, I led TRUSTe's development of the first privacy accreditation program for the consumer software industry, the Trusted Download Program ("TDP").⁴ This program included a broad range of stakeholders in its development, including industry (AOL, CNET, Verizon, Computer Associates, Yahoo!), independent think tanks and advocates such as the Center for Democracy and Technology. The program focused on:

1. A high bar of consumer disclosure, including key statements that would need to be elevated out of privacy policies and terms and conditions to more prominent placements in the pre-installation experience;
2. A prior consent requirement for advertising and tracking software;

¹ TRUSTe provides numerous services relating to consumer and website privacy, and has worked with companies such as Apple, AT&T, Cisco, Disney, eBay, HP and Intuit. Additional information can be found at www.truste.com. Additional information regarding privacy seals can be found at www.truste.com/products-and-services/enterprise-privacy/TRUSTed-websites.

² <http://www.returnpath.com/solution-silo/certification-eq/>

³ Additional information can be found at www.truste.com/products-and-services/enterprise-privacy/TRUSTed-email.

⁴ Additional information can be found at <http://www.truste.com/products-and-services/enterprise-privacy/TRUSTed-downloads>.

3. Tight controls for the distribution practices of program participants, including accountability for bad behavior detected across software bundling partners; and
4. A list of prohibited activities that all program participants would need to forswear.

TDP was launched to great acclaim, with Federal Trade Commissioner Jon Leibowitz appearing at the launch event, and TRUSTe quickly received applications from many of the leading advertising and research supported applications on the internet. It was in this capacity that I first became familiar with comScore applications, including their disclosures and the advanced steps the company has pursued to ensure consistent privacy practices across their distribution network.

I joined the TRUSTe executive team as Vice President of Strategic Partnerships and Programs after the launch of TDP, and the successful execution and market adoption across these privacy programs led to TRUSTe's first round of venture capital, with Accel partners contributing \$10 million.

In 2009, I left TRUSTe and co-founded Better Advertising (now 'Evidon'), another company focused on the privacy market for companies willing to adhere to best practices in consumer disclosure online. At Evidon, I have served as Chief Strategy Officer, leading Sales, Product Design, and Policy at various stages of the company's development. The company is backed by Warburg Pincus. Over a three year period Evidon became the leading technology provider for companies that sought to come into compliance with the enhanced disclosure requirements of the Self-Regulatory Principles for Online Behavioral Advertising,⁵ and the leading provider of ePrivacy Directive compliance services, which require companies to gain full consent for a wide range of tracking purposes. Evidon's clients include many of the leading marketers, publishers, and ad networks in the industry and its consumer disclosure technologies are served on top of 2 billion advertisements online every day.

Over the course of my nine years building technical systems in the online privacy space, I have regularly reached out to many of the leading voices in the privacy community to better understand their position on the issues and to ensure that the privacy systems I have built for my companies have a full picture of their compliance requirements. I have also become a public voice and educator on these issues.

My outreach has included:

- The Federal Trade Commission, including multiple Commissioners, the Chairman, the CTO, and staff
- Members of Congress
- Center for Democracy and Technology (CDT)
- Future of Privacy Forum (FPF)

⁵ Additional information can be found at www.aboutads.info.

- Staff from the European Commission
- The Information Commissioner and staff in the UK
- Which! (Consumer advocates in the UK)
- International Chamber of Commerce
- Data Protection Commissioner of Ireland and staff
- CNIL (French DPA)
- The Spanish Data Protection Agency
- Bavarian State Office for Data Protection
- The Japanese Ministry of Internal Affairs and Communications

My industry outreach has included regular speaking appearances and training programs at industry events, including the International Association of Privacy Professionals.

Recent bylines:

- AdMonsters: 'The Pragmatist's Guide to Compliance with the ePrivacy Directive'
 - <http://www.admonsters.com/blog/pragmatist's-guide-compliance-eprivacy-directive>
- Econsultancy: 'EU e-Privacy Directive: Don't Call it a Cookie Law' (5/2012)
 - <http://econsultancy.com/us/blog/9879-eu-e-privacy-directive-don-t-call-it-a-cookie-law>
- AOP: 'The Difference Between Consent and Opt-In' (4/2012)
 - <http://www.ukaop.org.uk/news/eu-privacy-directive-consent-opt-in-cookies-evidon3549.html>
- AOP: 'Why The Cookie Audit Rush?' (3/2012)
 - <http://www.ukaop.org.uk/news/how-to-run-a-cookie-audit3502.html>

My CV is attached to this report as Appendix A. I am being compensated at a rate of \$275 per hour for my work on this matter. I have not testified as an expert witness, either at deposition or trial, in the past four years.

Bases for Opinion

A list of the documents I reviewed while preparing my report is provided in Appendix B.

Opinion

It is my opinion that comScore's practices related to privacy disclosures and obtaining consent from users meet and exceed industry standards. Although it is impossible for any company to ensure that all users carefully consider privacy disclosures, and that all such users provide their consent in considered response to those disclosures, comScore has taken all commercially reasonable steps necessary to facilitate such careful consideration.

comScore Disclosures; Background and Assessment

comScore's Relevant Knowledge is a research application that tracks consumer behavior, including the pages viewed on the internet and setting sand application use across the operating system, in order to generate aggregated reports on general consumer trends. comScore does not offer any data service that would allow clients to target an individual, but nonetheless, the fact that individuals must be tracked to generate aggregated reports has required that comScore's software to monitor and collect a large amount of data. One of the central tenets of good privacy practice, and something that I have included in all of the disclosure systems I have designed over the last nine years, is the importance of providing clear and prominent notice when a company intends to collect and use a consumer's information in material ways that a typical consumer would not expect. Only when practices are held out in the light of day can consumers properly evaluate them. comScore has understood this well throughout the time that I have engaged with them, beginning in 2006.

When TRUSTe was designing the program requirements for the Trusted Download Program, we expected that applications like Relevant Knowledge would seek certification. Early on in the policy drafting process, we decided on a model that included the following core components:

- A **'Primary Notice,'** that would include the core components of the value proposition for the consumer in an unavoidable location, and for those 'Certified Tracking Software' applications like Relevant Knowledge, the notice would also include details regarding any collection, use, or transfer of PII.
- Users must be provided with a means to provide their **consent** having seen the Primary Notice, and we itemized specific requirements to ensure that language was direct, clear, and without any marketing gimmicks that might confuse or otherwise force unintended consent. Certified Tracking Software was subjected to additional requirements to ensure that the 'accept' button would not be the default option, to ensure that impatient consumers would have to pause and evaluate the value proposition before proceeding, and that the 'decline' option would be presented with equal prominence.
- Managing a large network of marketing partners online can be challenging for any business, and many large and reputable firms have struggled to do this effectively. But in the software distribution market, with applications that have potentially broad privileges on a consumer's machine, we felt at TRUSTe that we needed application owners to take accountability for the practices of their partners, particularly where the core privacy principles of the program were concerned. To this end, we created a section of the principles that we called **'Third Party Distribution/Affiliate Practices,'** that applied specifically to 'Certified Advertising Software' and 'Certified Tracking Software.' In this section, we included unprecedented requirements, including complete transparency for TRUSTe into the

individual partners and how each of them manage the installation process, and subjecting this list of partners to deep and ongoing scrutiny.

- Our requirements also included a long list of **'Prohibited Activities,'** including violations of the consumer's privacy rights or security settings and a range of potentially unscrupulous business practices. No application would be permitted to engage in these activities, with or without consumer consent.

comScore Disclosures

Relevant Knowledge is typically offered to a user in connection with the downloading of a partner's application. In this example, I will assess Relevant Knowledge as it appears in a bundle with the 'MP3 Cutter' application. It is my understanding and, accordingly I have assumed that, the process and disclosures are materially identical across all partner bundles.

Step 1: Consumer downloads MP3 Cutter

The consumer finds the MP3 Cutter application online and elects to download it.

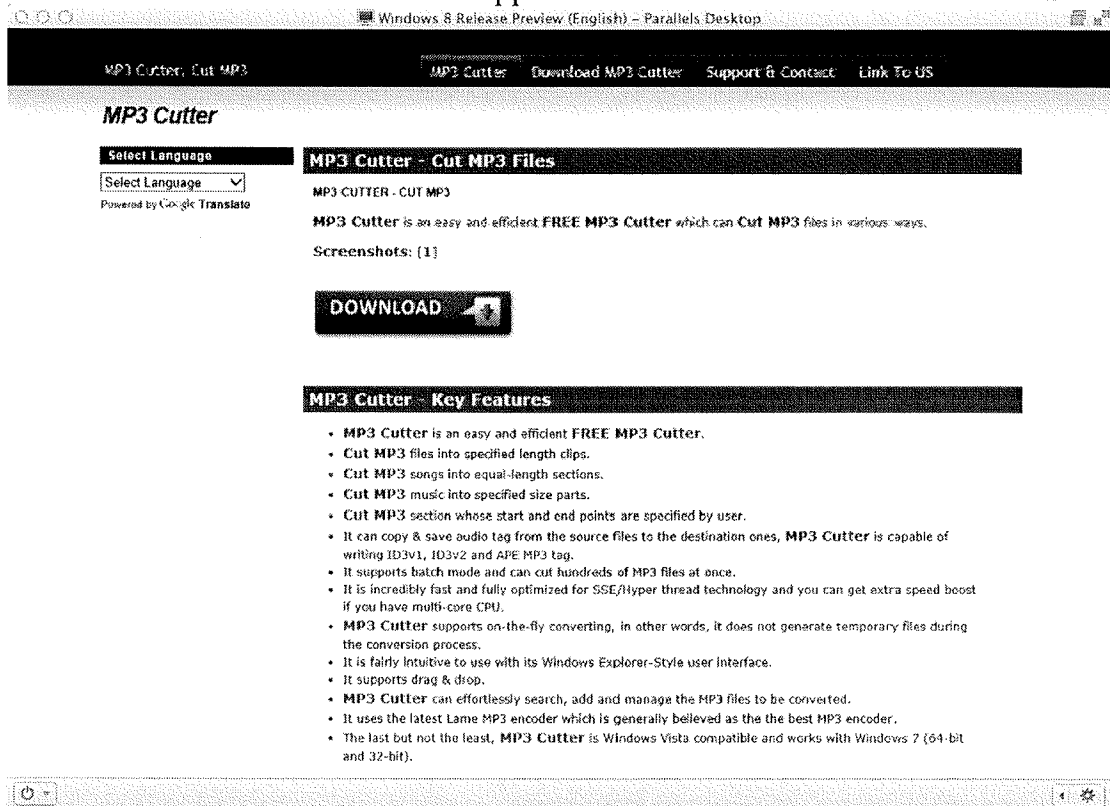


Image: MP3 Cutter download button

Step 2: Consumer begins MP3 Cutter installation

Once the download of MP3 Cutter is complete, the consumer finds the installation file and clicks to begin the installation process.

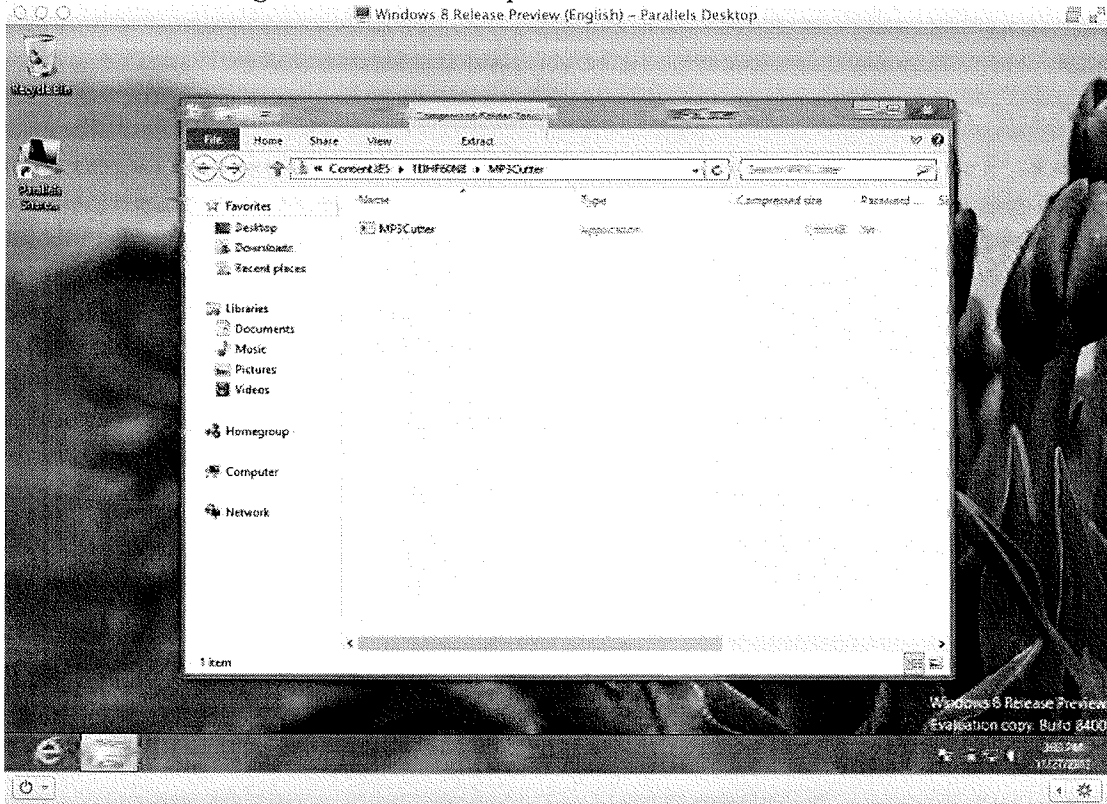


Image: MP3 Cutter installation file

Step 3: MP3 Cutter installer disclosure, including comScore 'WatchDog' reference, as explained below.

As the MP3 Cutter installation begins, MP3 Cutter has a chance to provide a disclosure to the consumer. In this case, comScore has worked with their partner to include a reference to their WatchDog application. WatchDog was created by comScore in order to meet the requirements of TDP. The sole purpose of WatchDog is to ensure that all consumers see the same comScore disclosures, that they are never hidden from view, and that consent is always properly obtained across their partner network. This purpose is accomplished through the use of a small application that is able to monitor the disclosure being presented—to assure that the approved disclosure is being presented in its entirety—and that each consumer selects the “accept” option. If WatchDog detects that either of these events did not occur, then the comScore software will not be installed. The WatchDog thus acts as a privacy security offering, and is one example of comScore going beyond TRUSTe requirements.

The MP3 Cutter reference does not mention WatchDog or comScore by name, as this would likely confuse the consumer, but it mentions that the application is from a partner, that its purpose is to verify acceptance of disclosures, and that it will be promptly removed. This disclosure is presented wherever possible before WatchDog is installed, in keeping with best practices.

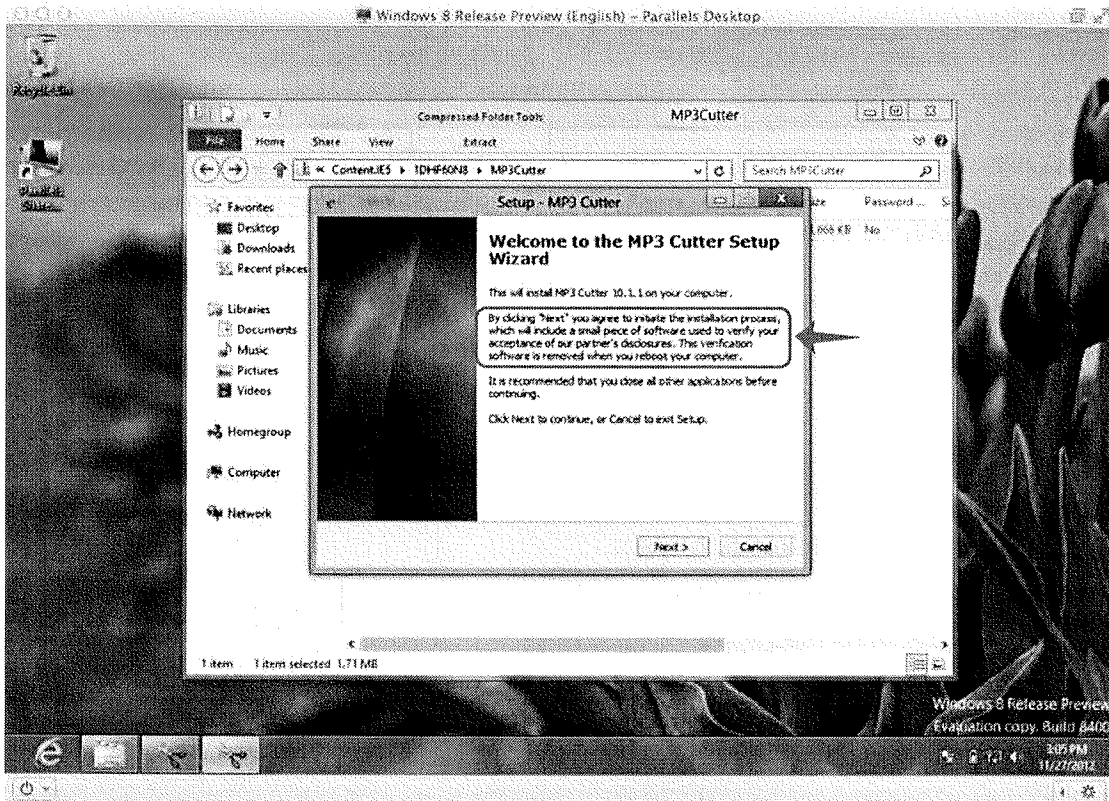


Image: MP3 Cutter disclosure with comScore WatchDog reference (orange highlights for effect, not in original)

Step 4: MP3 Cutter Terms

MP3 Cutter then presents it's terms of service to the consumer and requests consent.

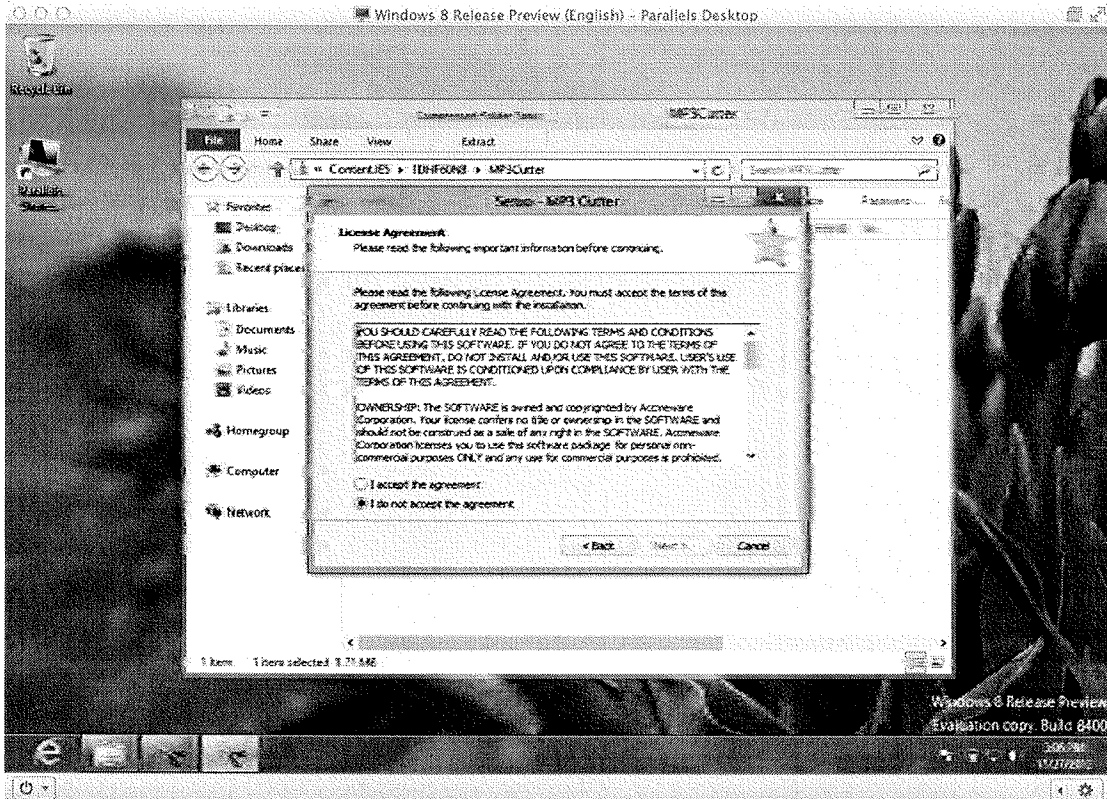


Image: MP3 Cutter terms of service with consent dialogue

Step 5: Relevant Knowledge Primary Notice

With the MP3 Cutter disclosures complete, Relevant Knowledge now presents its Primary Notice, which is the most important dialogue to the user. This notice was originally drafted in conjunction with TRUSTe, and as such is fully compliant with TRUSTe's Trusted Download Program requirements, and accomplishes several important things:

1. **Headline:** The consumer is informed that MP3 Cutter is part of a software bundle.
2. **Value Proposition Presented:** Relevant Knowledge is described, including the company behind the application and the core business model and value proposition.
3. **Tracking Disclosed:** A complete description of the tracking that will take place is provided, including how the data will be used.
4. **All Essential Information Immediately Visible:** Enough information is provided to outline the core value proposition without requiring the

consumer to advance to any secondary screen or having to scroll to see additional information beyond that which is immediately visible in the Primary Notice.

5. **Additional Legal Documents Immediately Accessible:** Links are provided to the Privacy Policy and User License Agreement for more detailed information.⁶
6. **No Bias Towards 'Accept':** 'Accept' is NOT highlighted as a default option or otherwise marketed in any way as a more desirable option than 'Decline.'
7. **User Must Make an Active Decision:** The 'Next' button is not active until the user selects Accept or Decline, so the impatient consumer that simply wants to hit 'Enter' will not be able to proceed without making a decision.
8. **Decline is a Viable Option:** If the consumer elects to Decline, Relevant Knowledge will not be installed, and MP3 Cutter will remain on their machine. They are not forced to agree to Relevant Knowledge terms to obtain MP3 Cutter. This again exceeds the requirements of TRUSTe's Trusted Download Program.

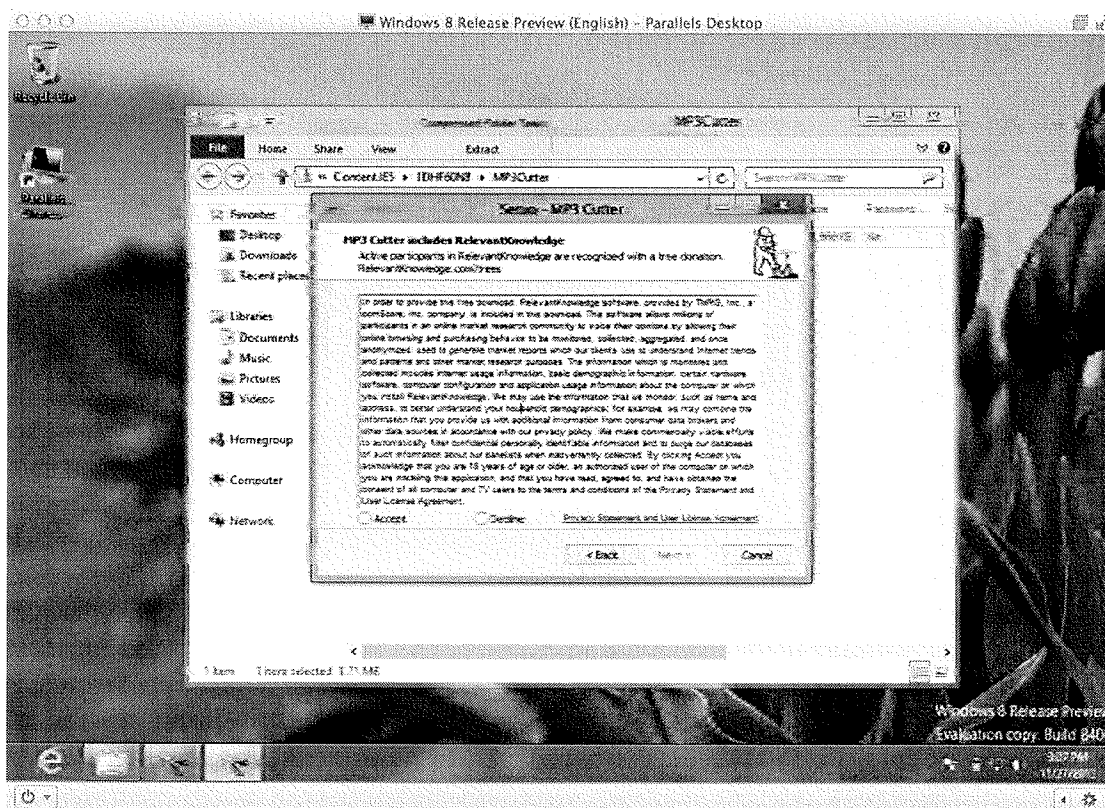


Image: Relevant Knowledge Primary Notice⁷

⁶ It is my understanding that one of comScore's partners inadvertently failed to include a link to comScore's Privacy Policy and User License Agreement in the Primary Notice for a short period of time. Such a link is not required to obtain adequate consent from a user, and comScore corrected the issue in partnership with its partner as soon as it was made aware of the issue.

⁷ The notice as reproduced here is smaller than actual size.

Relevant Knowledge is only installed if the user accepts the terms and clicks 'Next.'

In summary, the notice adheres to best practices as outlined by TRUSTe's Trusted Download Program, and exceeds them in several critical places where comScore has innovated to increase confidence that consumer consent is legitimately obtained.

The Relevant Knowledge Notice Assessed Against Digital Advertising Alliance Online Behavioral Advertising Standards

The Digital Advertising Alliance⁸ ("DAA") is a trade association that is operated in coordination with the major sector based associations across the online marketing ecosystem, including the IAB, DMA, AAAA, ANA, AAF, NAI, and the BBB. In 2009, the DAA released a set of standards for consumer privacy in the online behavioral advertising space ("OBA") that is notable for its broad adoption (more than 1 trillion notices served every month⁹) and governmental support, including the FTC¹⁰ and the White House.¹¹ The principles, titled Self-Regulatory Principles for Online Behavioral Advertising,¹² are useful for assessing the sufficiency of notice, because they are reasonably specific about where and how notice should be provided, and when additional consent mechanisms should be in place.

To be clear, comScore does not engage in behavioral advertising with data collected through Relevant Knowledge, so I intend to use these principles as a reference point only, without implying that the program imposes direct requirements on comScore.

The DAA's principles require that third parties collecting information about consumers across websites (and for the purpose of behavioral advertising), provide notice to consumers when this data collection and use is taking place in an easily visible location, and a means to control the tracking activity.

In addition, the DAA creates a category of company called 'Service Providers' with a scope that is similar to TRUSTe's 'Certified Tracking Software.'

A Service Provider is defined as an entity to the extent that it collects and uses data from all or substantially all URLs traversed by a web browser across Web sites for Online Behavioral Advertising in the course of its activities as a provider of Internet access service, a toolbar, an Internet browser, or comparable desktop application or client software and not for its other applications and activities.

⁸ <http://www.aboutads.info>

⁹ <http://adage.com/article/digital/daa-takes-aim-microsoft-congressional-hearing/235688/>

¹⁰ http://www.imediaconnection.com/article_full.aspx?id=30430

¹¹ <http://www.prnewswire.com/news-releases/white-house-doc-and-ftc-commend-daas-self-regulatory-program-to-protect-consumer-online-privacy-140170013.html>

¹² <http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf>

Service Providers have important additional requirements, and while again, comScore does not use Relevant Knowledge data for OBA, and therefore does not meet the definitional threshold, the standards are instructive.

In particular, Service Providers must:

- Adhere to **strict prior consent**. The DAA requires that companies in this category refrain from using data for itemized purposes until consent has been granted. comScore uses this model explicitly through the tightly controlled consent process discussed in the previous section.¹³
- **Honor a high bar for Consent**, which is defined as follows:

The term Consent means an individual's action in response to a clear, meaningful and prominent notice regarding the collection and use of data [for Online Behavioral Advertising purposes].

comScore's notice, as described above, clearly meets this requirement.

- Allow the consumer to **withdraw consent at any time**.¹⁴ comScore adheres to this principle by combining visual reminders that the application is running and/or resident on the consumer's computer, and also by ensuring that it is visible wherever possible in the add/remove programs section of the operating system, as seen below.

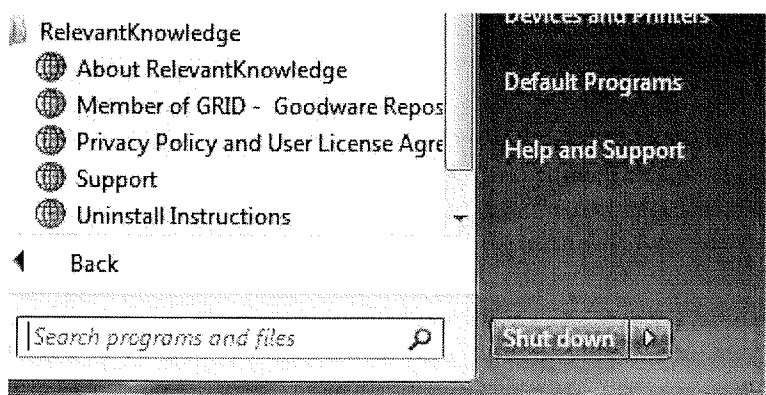


Image: Relevant Knowledge in the Start Menu

¹³ III. Consumer Control: B. Service Provider Consent for Behavioral Advertising: 1. Consent to Collection and Use

¹⁴ III. Consumer Control: B. Service Provider Consent for Behavioral Advertising: 2. Withdrawing Consent

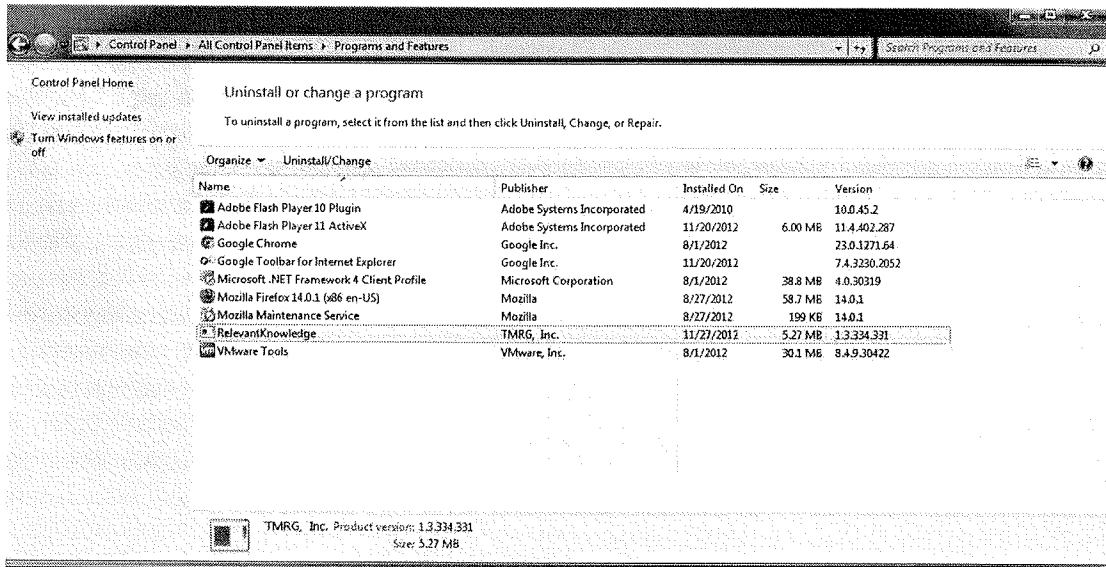


Image: Relevant Knowledge in Add/Remove Programs

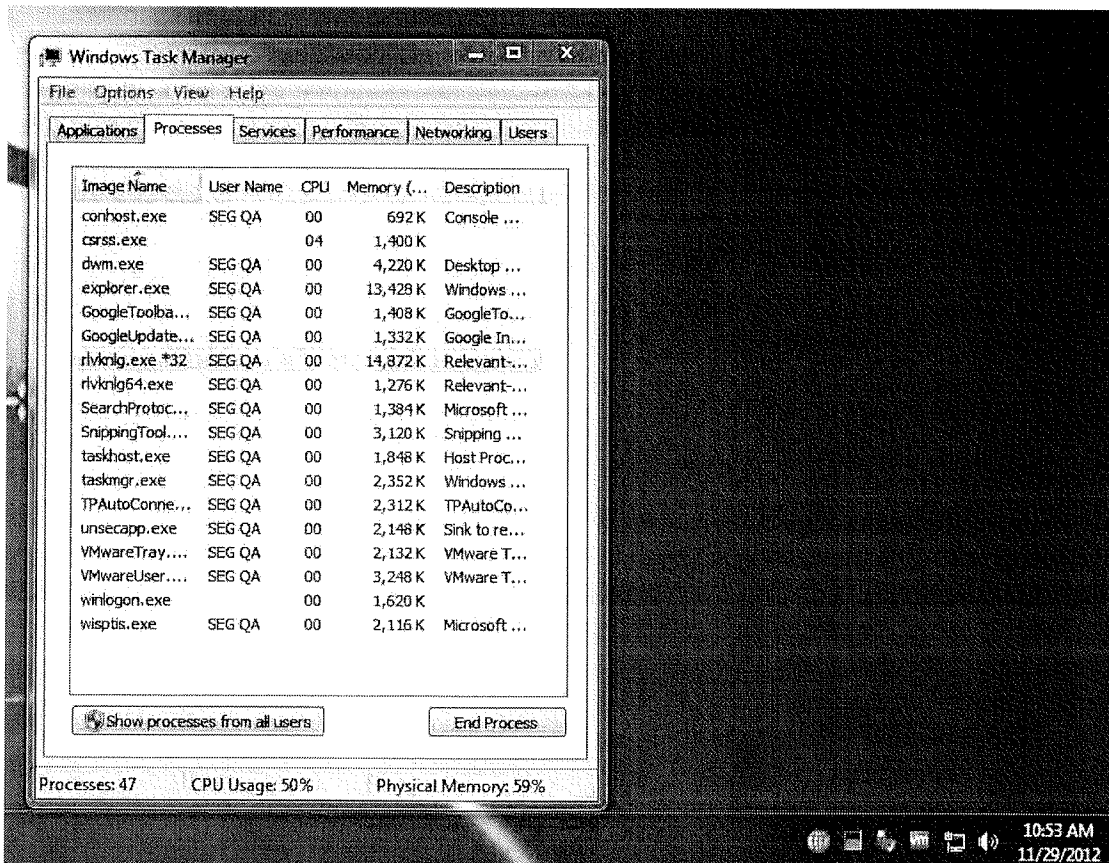


Image: Relevant Knowledge in Task Manager

- Adhere to specific requirements to anonymize and secure consumer data,¹⁵ through the use of comScore’s fuzzification process.¹⁶
 1. *Alter, anonymize, or randomize (e.g., through “hashing” or substantial redaction) any PII or unique identifier in order to prevent the data from being reconstructed into its original form in the ordinary course of business.*
 2. *Disclose in the notice set forth in II.A.1 the circumstances in which data that is collected and used for Online Behavioral Advertising is subject to such a process.*
 3. *Take reasonable steps to protect the non-identifiable nature of data if it is distributed to non-Affiliates including not disclosing the algorithm or other mechanism used for anonymizing or randomizing the data, and obtaining satisfactory written assurance that such entities will not attempt to re-construct the data and will use or disclose the anonymized data only for purposes of Online Behavioral Advertising or other uses as specified to users. This assurance is considered met if a non-Affiliate does not have any independent right to use the data for its own purposes under a written contract.*
 4. *Take reasonable steps to ensure that any non-Affiliate that receives anonymized data will itself ensure that any further non-Affiliate entities to which such data is disclosed agree to restrictions and conditions set forth in this subsection. This obligation is also considered met if a non-Affiliate does not have any independent right to use the data for its own purposes under a written contract.*

Relevant Knowledge Compared to Other Commercial Examples

Relevant Knowledge uses a prior consent model that compares favorably to similar methods used by many of the leading companies conducting business on the internet. In this section, I will examine a series of examples from companies in related industries and assess how they meet the eight criteria that we outlined for Relevant Knowledge above.

¹⁵ IV. Data Security: C. Service Provider Treatment of Online Behavioral Advertising Data

¹⁶ It is my understanding that comScore’s fuzzification process is the subject of a separate expert report, and thus will not be covered here in great detail. My understanding of the process is that when comScore’s software is able to identify PII, the software affects changes to that data prior to the data being sent to comScore’s servers. Additionally, comScore takes steps to assure that any data collected is transmitted at the same level of security to which the underlying data was subject. Thus, data collected from secure pages will be transmitted across a secure (https) connection back to comScore’s servers, even if the data has previously been hashed or otherwise redacted. It is also my understanding that this process is completely controlled by comScore, and does not rely in any amount of the efforts of their distribution network.

A. Microsoft's Silverlight

Silverlight is a multimedia playing application that allows the consumer to playback certain forms of audio and video content. Certain information is presumably collected by Microsoft about the consumer's computer and the content they are viewing to properly maintain the service, though this is not immediately clear in the portion of the notice that is immediately viewable. Microsoft does disclose that they will update the application automatically without necessarily notifying the consumer.

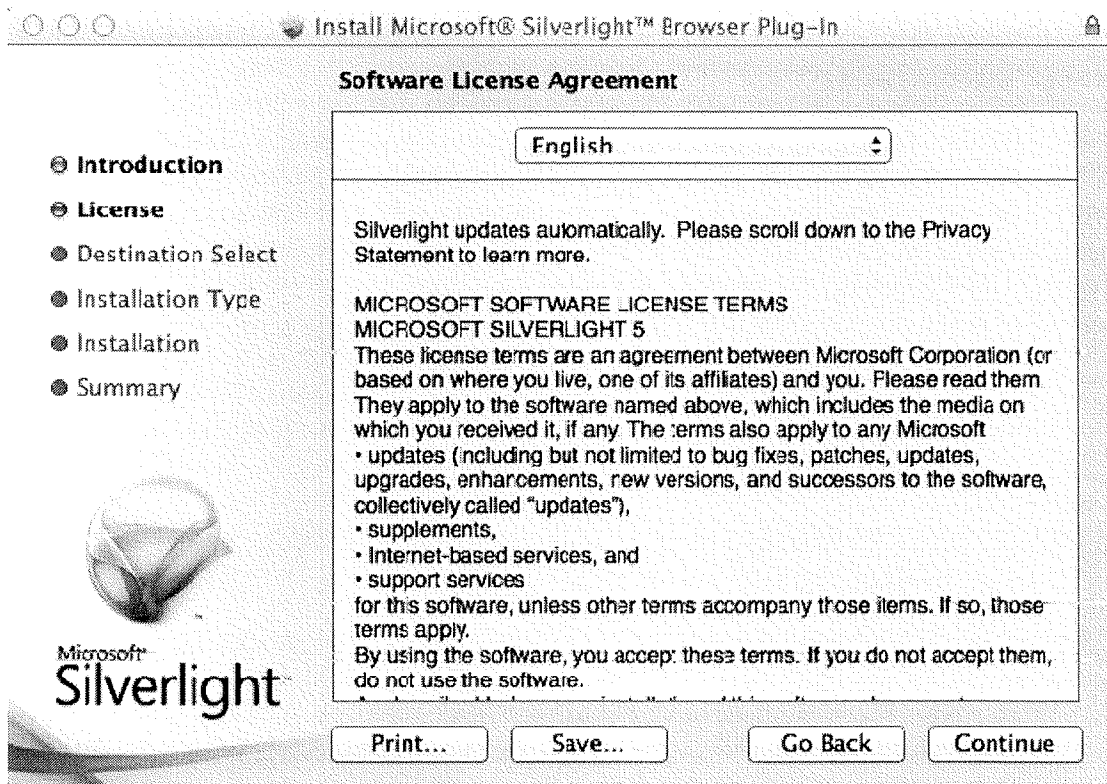


Image: Microsoft Silverlight notice

1. **Headline:** Clearly states the name of the application and the company behind it.
2. **Value Proposition Presented:** The disclosure does not include a description of the behavior of the application or the underlying business model.
3. **Tracking Disclosed:** No tracking is disclosed.
4. **All Essential Information Immediately Visible:** No, and it is clear that additional information is hidden beneath the fold.
5. **Additional Legal Documents Immediately Accessible:** No, and in particular, there is no Privacy Policy link.
6. **No Bias Towards 'Accept':** Yes.

7. **User Must Make an Active Decision:** Yes.
8. **Decline is a Viable Option:** No, if you do not accept by selecting 'Continue,' you will not receive the application.

B. Adobe Reader

Adobe Reader is a free application that allows the consumer to read PDF documents.

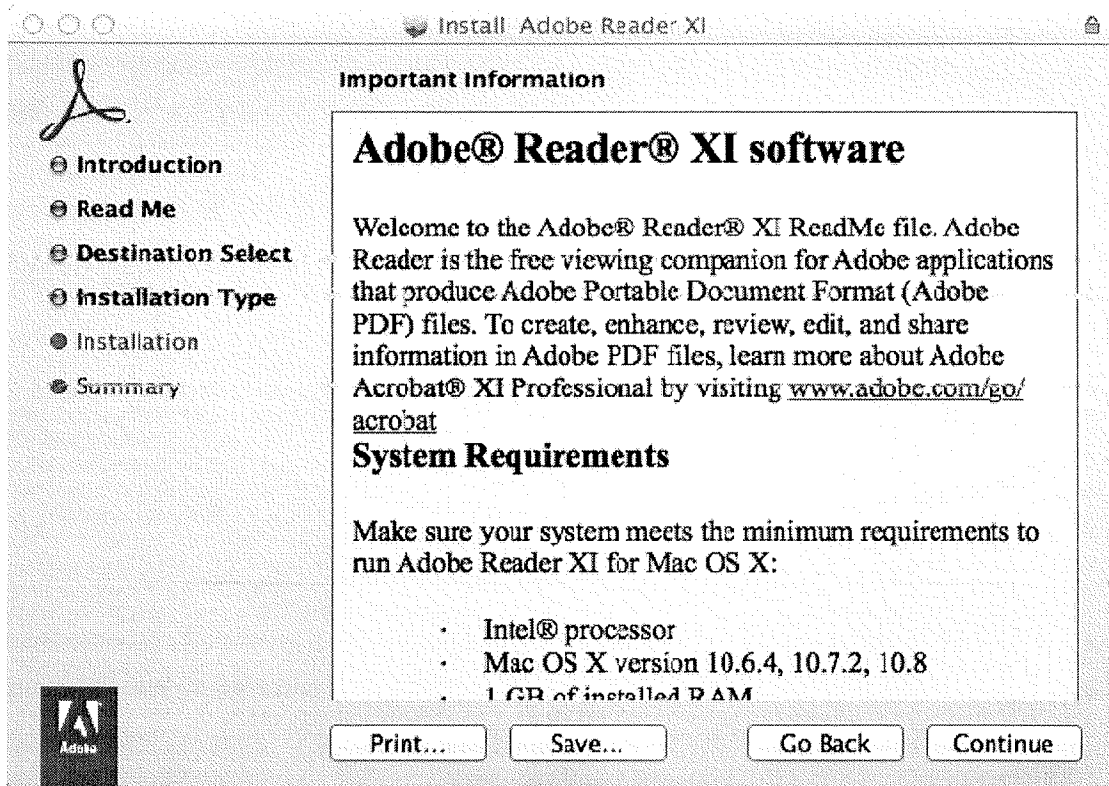


Image: Adobe Reader notice page 1

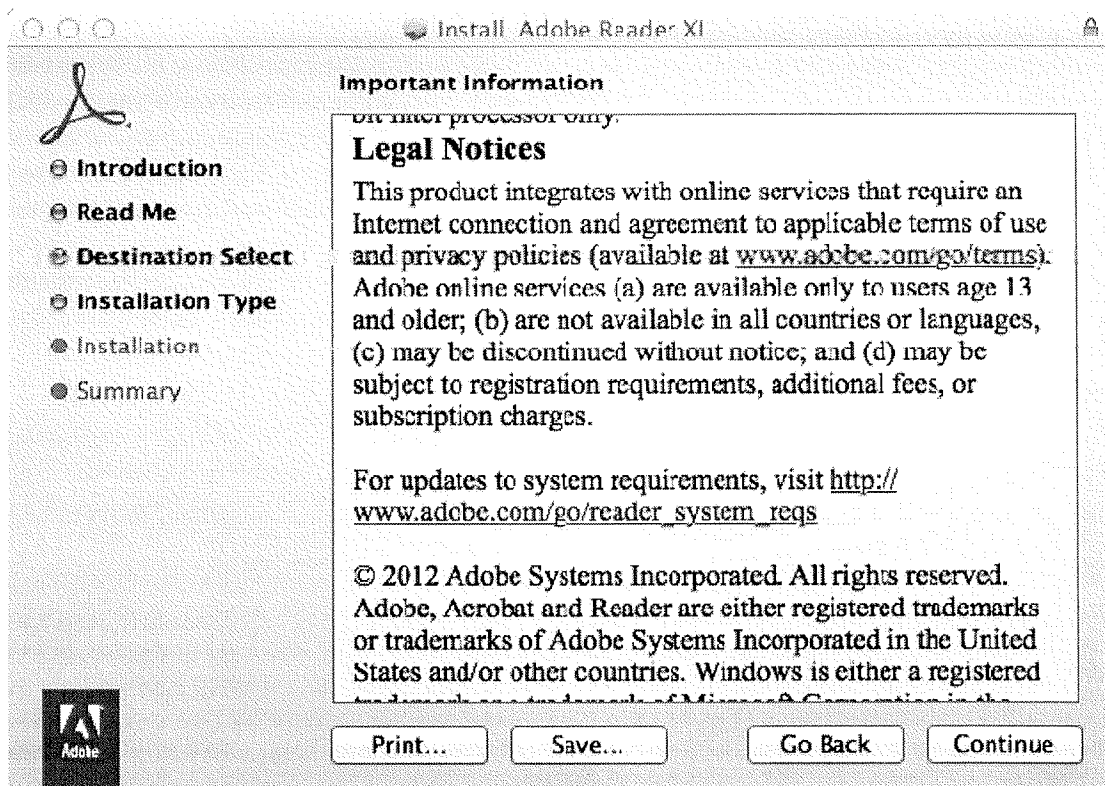


Image: Adobe Reader notice page 2, after scroll

1. **Headline:** Adobe and Adobe reader are clearly declared.
2. **Value Proposition Presented:** The core function of the application is clearly disclosed at the top of the first paragraph.
3. **Tracking Disclosed:** No, though it's possible that no tracking takes place other than what a consumer would expect from a similarly situated application.
4. **All Essential Information Immediately Visible:** Yes.
5. **Additional Legal Documents Immediately Accessible:** No, as legal links like the 'Terms' page are hidden beneath the fold and a scroll is required.
6. **No Bias Towards 'Accept':** Yes
7. **User Must Make an Active Decision:** Yes
8. **Decline is a Viable Option:** No

C. Reuter's Cookie Consent in the UK

As a result of the ePrivacy Directive, websites in the UK are required by law to obtain consent from each consumer in order to track them for a variety of common commercial purposes, including research, ongoing product improvement, analytics, and behavioral advertising. As a result, companies like Reuters have developed disclosure systems that ensure

each consumer sees the requisite information and has the ability to revoke consent if they are inclined. The particular interface shown below is provided by my company, Evidon.

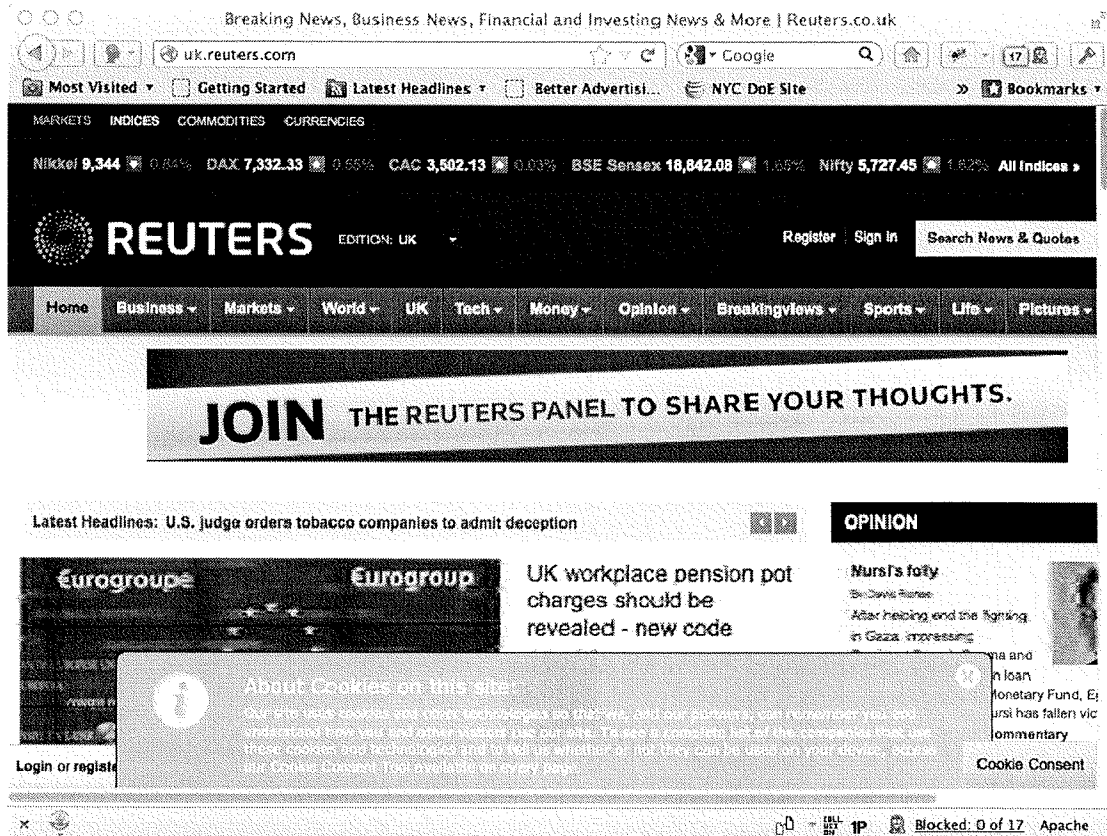


Image: Reuters UK consent interface

1. **Headline:** Properly notifies the consumer that the notice pertains to cookies.
2. **Value Proposition Presented:** Quickly summarized in a short paragraph.
3. **Tracking Disclosed:** Yes.
4. **All Essential Information Immediately Visible:** Yes.
5. **Additional Legal Documents Immediately Accessible:** The 'Cookie Consent' button contains additional legal documents.
6. **No Bias Towards 'Accept':** There is a clear bias towards 'Accept,' as this is an implied consent model that presumes the consumer's consent unless it is revoked through the 'Cookie Consent' button.
7. **User Must Make an Active Decision:** Yes, as the consumer must continue to use the site, having seen the value proposition, and its included tracking.
8. **Decline is a Viable Option:** Yes, as the consumer can withdraw consent through the 'Cookie Consent' button.

D. BBC Cookie Consent in the UK

The BBC has developed a consent interface for their website that is similar to Reuters to meet the requirements of the ePrivacy Directive in the UK.

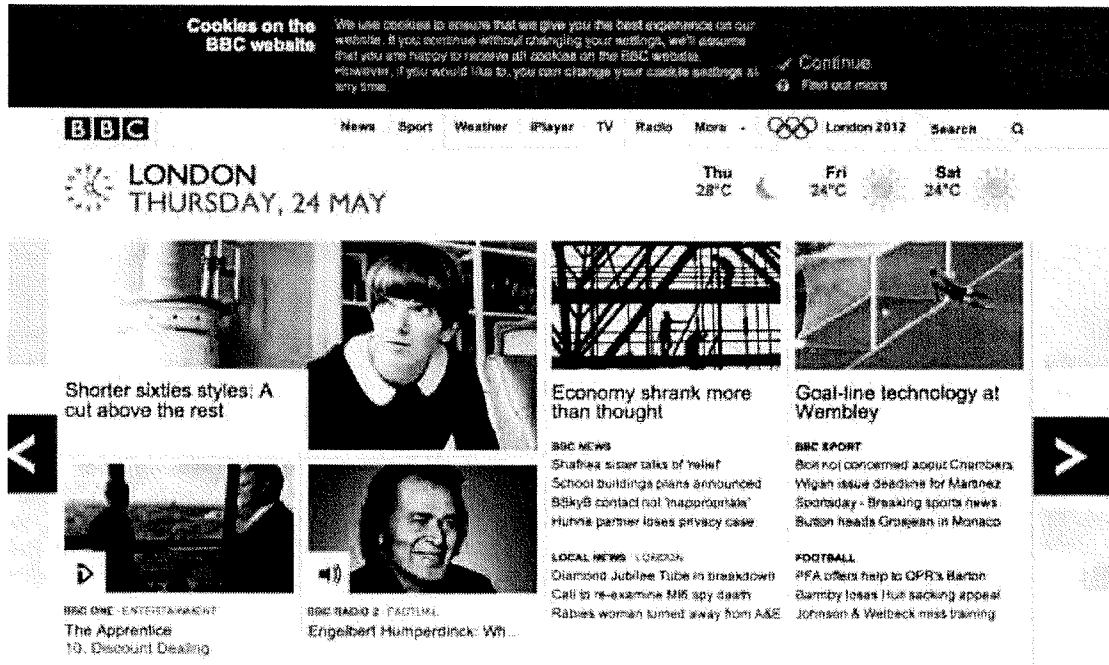


Image: BBC consent interface

1. **Headline:** Properly notifies the consumer that the notice pertains to cookies.
2. **Value Proposition Presented:** Quickly summarized in a short paragraph.
3. **Tracking Disclosed:** Yes.
4. **All Essential Information Immediately Visible:** Yes.
5. **Additional Legal Documents Immediately Accessible:** The 'Find out more' link will take the consumer to additional legal documents.
6. **No Bias Towards 'Accept':** There is a clear bias towards 'Accept,' as this is an implied consent model that presumes the consumer's consent unless it is revoked through the 'Change your cookie settings' link.
7. **User Must Make an Active Decision:** Yes, as the consumer must continue to use the site, having seen the value proposition, and it's included tracking.
8. **Decline is a Viable Option:** Yes, as the consumer can withdraw consent through the 'Change your cookie settings' link.

E. Chase Credit Card Agreement

Chase provides an online application process for credit cards. Once the account is established, Chase has the right to track the consumer's use of the card for a variety of purposes, ranging from security to marketing, and the application is also a financial contract in a tightly regulated industry. The image below is taken from the section of the application that presents core terms along with the 'Submit' button to proceed with the application, with the consumer presumed to have understood the terms.

The screenshot shows a web browser window titled "Chase Credit Card Application". The address bar shows the URL "https://applynow.chase.com/FlexAppWeb/renderApp.do?CELL=34". The page content includes a "Pricing & Terms" section with a "Print" button. Below this is a "PRICING INFORMATION" section containing a scrollable box titled "INTEREST RATES AND INTEREST CHARGES".

INTEREST RATES AND INTEREST CHARGES	
Purchase Annual Percentage Rate (APR)	0% Intro APR for the first 15 billing cycles that your Account is open. After that, 12.99% to 22.99%, based on your creditworthiness. These APRs will vary with the market based on the Prime Rate. ³
Balance	0% Intro APR for the first 15 billing cycles that your Account is open.

Below the pricing information is an "AUTHORIZATION" section with a list of terms and conditions. At the bottom of the authorization section is a "SUBMIT" button. The page footer includes "For Bank Use Only" and "Help, Staff".

Image: Chase Credit Card Terms

1. **Headline:** Very clear.
2. **Value Proposition Presented:** Yes.
3. **Tracking Disclosed:** Not entirely clear.
4. **All Essential Information Immediately Visible:** No, most of the core terms lie in the scroll box, hidden from immediate view.
5. **Additional Legal Documents Immediately Accessible:** Yes.
6. **No Bias Towards 'Accept':** No, as you must accept to proceed.
7. **User Must Make an Active Decision:** Yes.

8. **Decline is a Viable Option:** No.

F. Nickelodeon

Nickelodeon operates a website that is designed to cater to both children and their parents, and as such, it is subject to additional scrutiny and legal requirements, including those imposed by the Children's Online Privacy Protection Act ("COPPA"). Here I'll assess their quality of notice using the Relevant Knowledge standard in two forms, one for the DAA's OBA program, and then consent as the consumer registers and Nickelodeon establishes its COPPA compliance.

- i) **OBA Compliance:** The first time a consumer arrives on the Nickelodeon homepage, Nickelodeon allows a series of third party companies to drop cookies and use related technologies that may be used for online behavioral advertising. As a result of this tracking activity, the DAA would require that Nickelodeon include notice on the page with a link to an opt-out tool. Nickelodeon satisfies this requirement by including a link with an icon using the text 'Ad Choices' at the bottom of the page, visible after a full scroll. When a consumer clicks through on this link, they are taken to a page operated by Nickelodeon's parent company, Viacom, where the tracking activity is disclosed and a further link is provided to a site operated by a third brand, this time the DAA, where an opt-out can be processed.



Image: Nickelodeon initial homepage

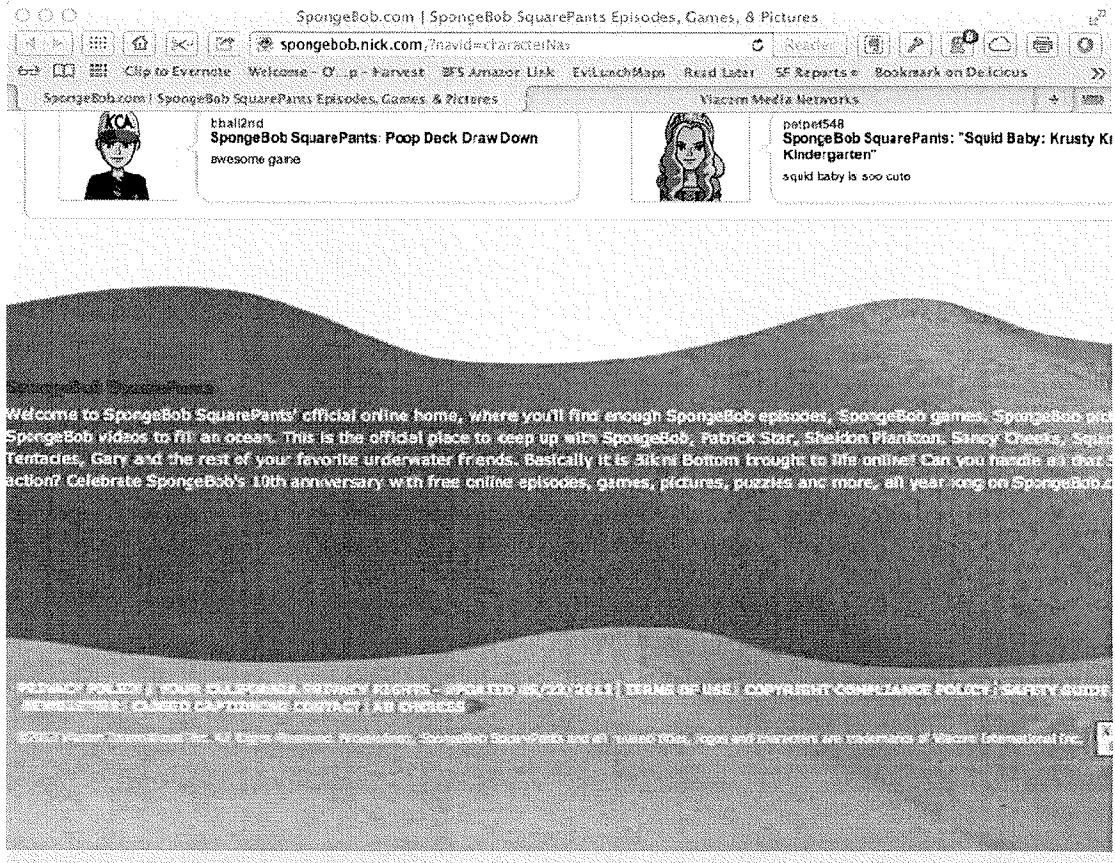


Image: Nickelodeon homepage, beneath the fold, showing 'Ad Choices' link in footer

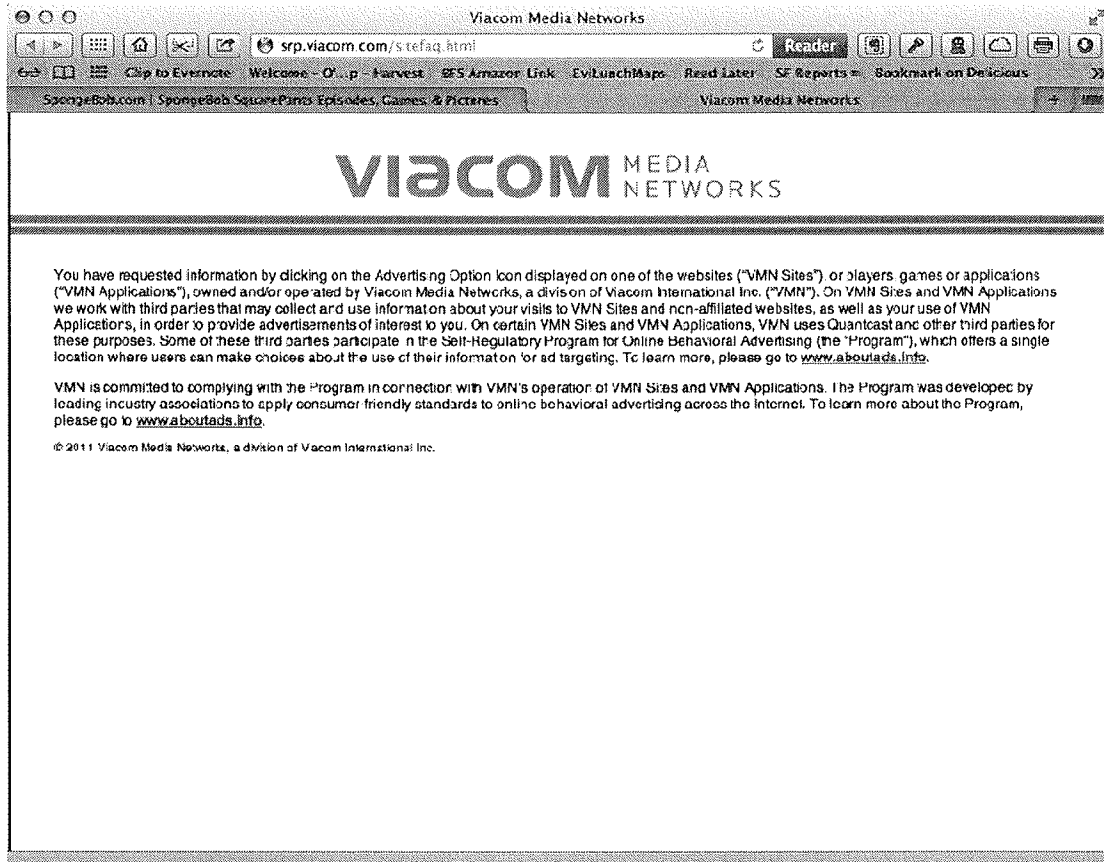


Image: Nickelodeon parent company, Viacom Media Networks OBA Compliance page

1. **Headline:** Ad Choices, which is not entirely clear to the consumer.
2. **Value Proposition Presented:** Yes, but only after an initial click.
3. **Tracking Disclosed:** Yes, but only after an initial click.
4. **All Essential Information Immediately Visible:** No.
5. **Additional Legal Documents Immediately Accessible:** No.
6. **No Bias Towards 'Accept':** No, Nickelodeon is not using a consent standard, and tracking will continue unless the consumer objects.
7. **User Must Make an Active Decision:** No.
8. **Decline is a Viable Option:** Yes, as the consumer can opt-out.

ii) **Site Registration:**

To establish a registered account and 'Join the Club' at Nickelodeon, consumers fill out a form online. The form includes critical fields, including the birthday of the user, which allows the site to comply with legal requirements imposed by COPPA, and asks the consumer to confirm that they have read two separate legal documents, the 'Privacy Policy/Your California Privacy Rights,' and 'Terms of Use.'

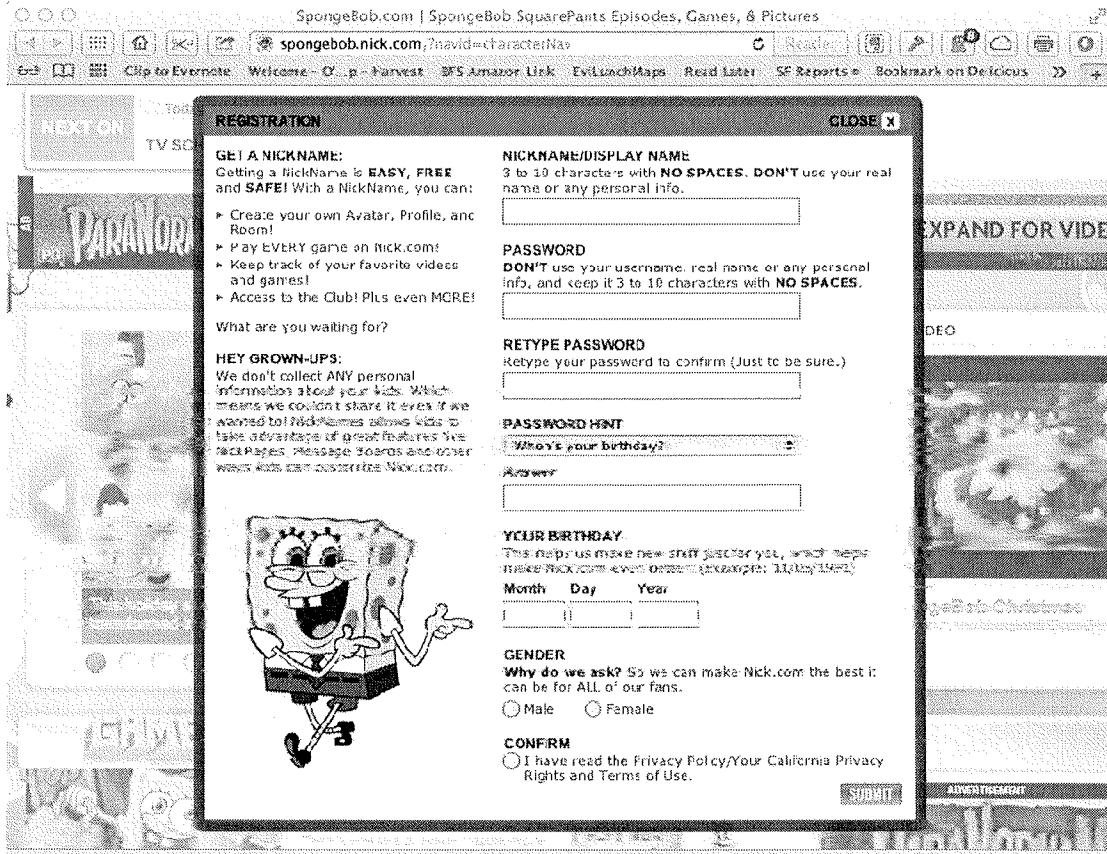


Image: Nickelodeon registration form

1. **Headline:** Very clear.
2. **Value Proposition Presented:** Yes.
3. **Tracking Disclosed:** No, though the site tracking implemented by Nickelodeon may be less relevant in this context.
4. **All Essential Information Immediately Visible:** Yes.
5. **Additional Legal Documents Immediately Accessible:** Yes.
6. **No Bias Towards 'Accept':** No, as there is no alternative to 'I have read the Privacy Policy,' etc. This form moves beyond a bias, and forces the user to tell Nickelodeon the answer it wants to hear.
7. **User Must Make an Active Decision:** Yes.
8. **Decline is a Viable Option:** No, as above.

G. US Department of Homeland Security Global Entry Program Consent for Monitoring

The GOES system is a US Federal Government initiative to provide for expedited border crossing for registered citizens, among other priorities. The US Department of Homeland Security is responsible for the system, and monitors its use in various ways to guard against misuse and for other security purposes. It is possible that this monitoring could lead to a

direct legal or security-oriented action against the user of the site. With the stakes this high, the Department determined that it should request consumer consent.

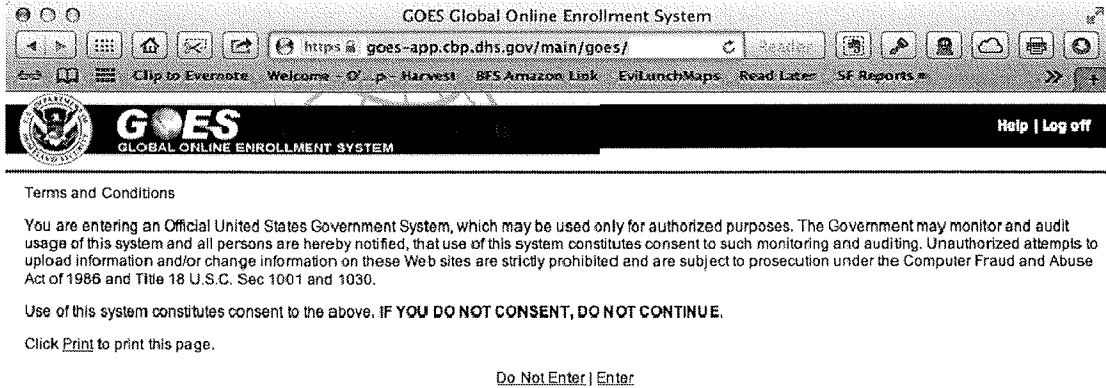


Image: GOES notice page 1

1. **Headline:** Unclear, as this is really a consent for tracking interface rather than a traditional 'Terms and Conditions' document.
2. **Value Proposition Presented:** No.
3. **Tracking Disclosed:** Yes.
4. **All Essential Information Immediately Visible:** No. In particular, the Department never discloses what kind of information will be collected and what purposes the information will be used for.
5. **Additional Legal Documents Immediately Accessible:** No.
6. **No Bias Towards 'Accept':** No, as this is another example where 'Accept' is the ONLY option.
7. **User Must Make an Active Decision:** Yes.
8. **Decline is a Viable Option:** No.

H. Safeway Loyalty Program Registration

A Safeway club card is part of a loyalty program that includes significant tracking activity. Safeway will track all of the consumer's purchases once they establish their club account, and will use this data to, among other things, send the consumer individualized marketing materials.

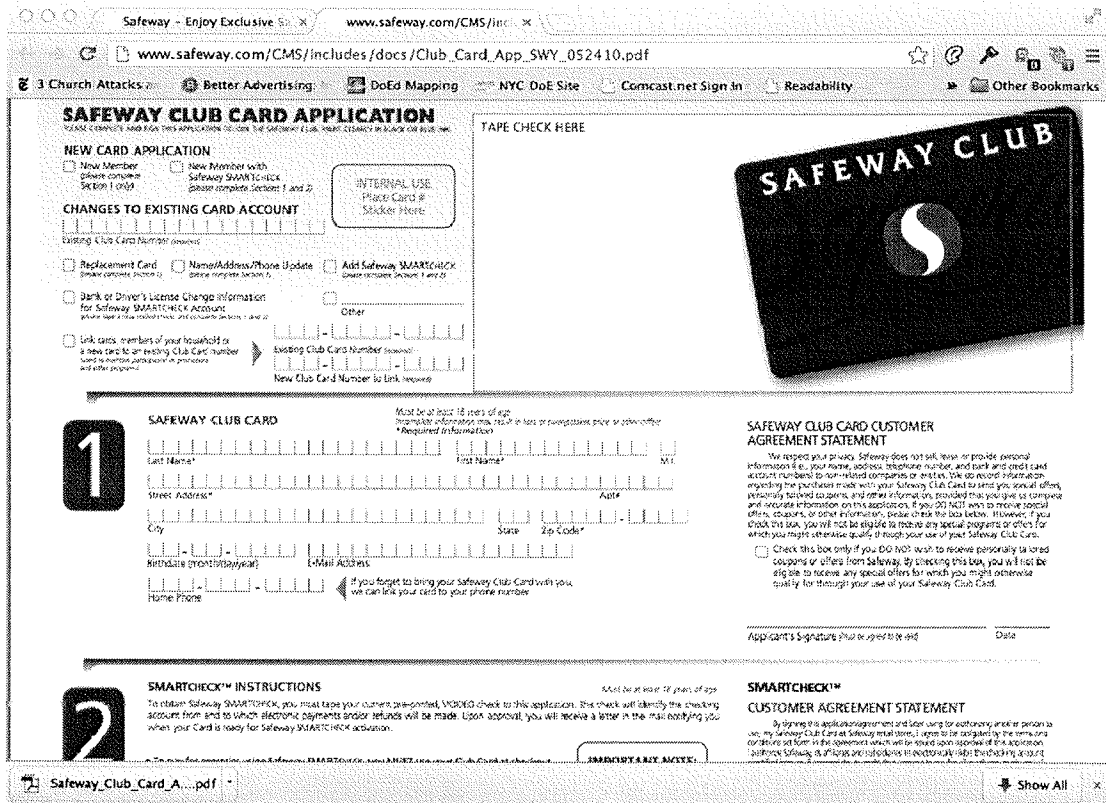


Image: Safeway Club Card Application

1. **Headline:** Very clear.
2. **Value Proposition Presented:** Yes.
3. **Tracking Disclosed:** Yes.
4. **All Essential Information Immediately Visible:** Yes.
5. **Additional Legal Documents Immediately Accessible:** No, though this is difficult to accomplish in an offline form.
6. **No Bias Towards 'Accept':** No, as the consumer's consent is presumed unless they check 'Do Not wish to receive ...' box.
7. **User Must Make an Active Decision:** Yes, as you must fill out the form.
8. **Decline is a Viable Option:** Yes.

I. Apple Location-based Service Enablement Disclosure

Apple prompts the user whenever an application in iOS (the Apple mobile operating system) would like to use specific location information about the consumer. Precise location information is a very sensitive category of data according to many privacy advocates and trade associations alike, so whereas iOS regularly provides information about the consumer's device to application owners without consent (time, browser, version of the operating system, language, etc.), Apple has built a unique consent experience where specific location information is requested. In this case,

we are seeing the consent interface in a situation where an application also owned by Apple (Safari), is requesting location information.

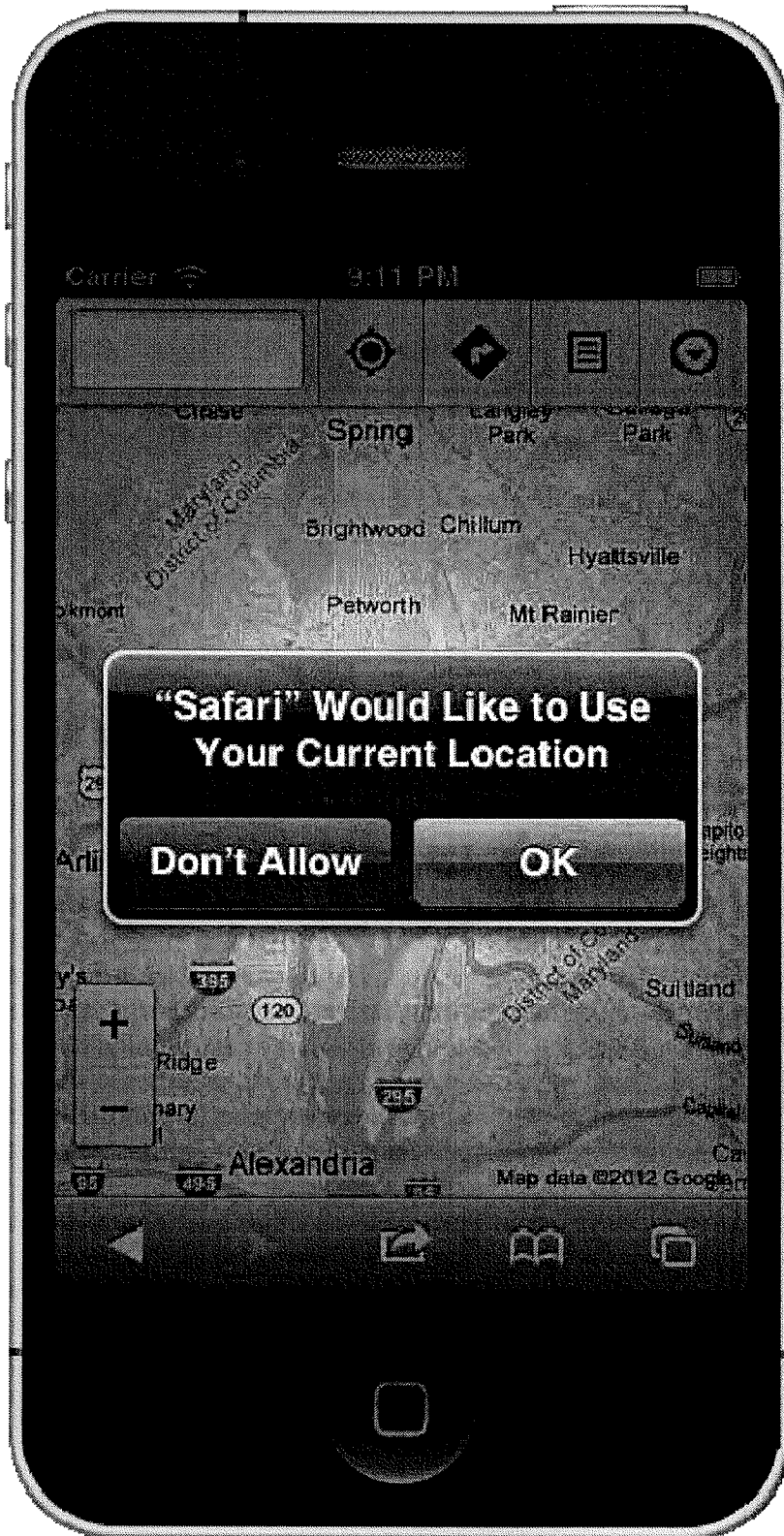


Image: Safari Location "Pop"

1. **Headline:** Very clear.
2. **Value Proposition Presented:** No, there is no written context, though these alerts are shown as 'just in time' notices, meaning that they are prompted by the application's real time request for location information. In many cases, the consumer is therefore able to infer the context and overall value proposition.
3. **Tracking Disclosed:** Yes.
4. **All Essential Information Immediately Visible:** Yes.
5. **Additional Legal Documents Immediately Accessible:** No.
6. **No Bias Towards 'Accept':** No, as 'Ok' is the highlighted option.
7. **User Must Make an Active Decision:** Yes.
8. **Decline is a Viable Option:** Yes.

J. Google Toolbar Disclosure

- i) Google Toolbar creates an embedded Google search interface in your browser and includes tie-ins to many other Google services. When you install the toolbar, Google also attempts adjust important settings within your browser, including your default search engine and your homepage.

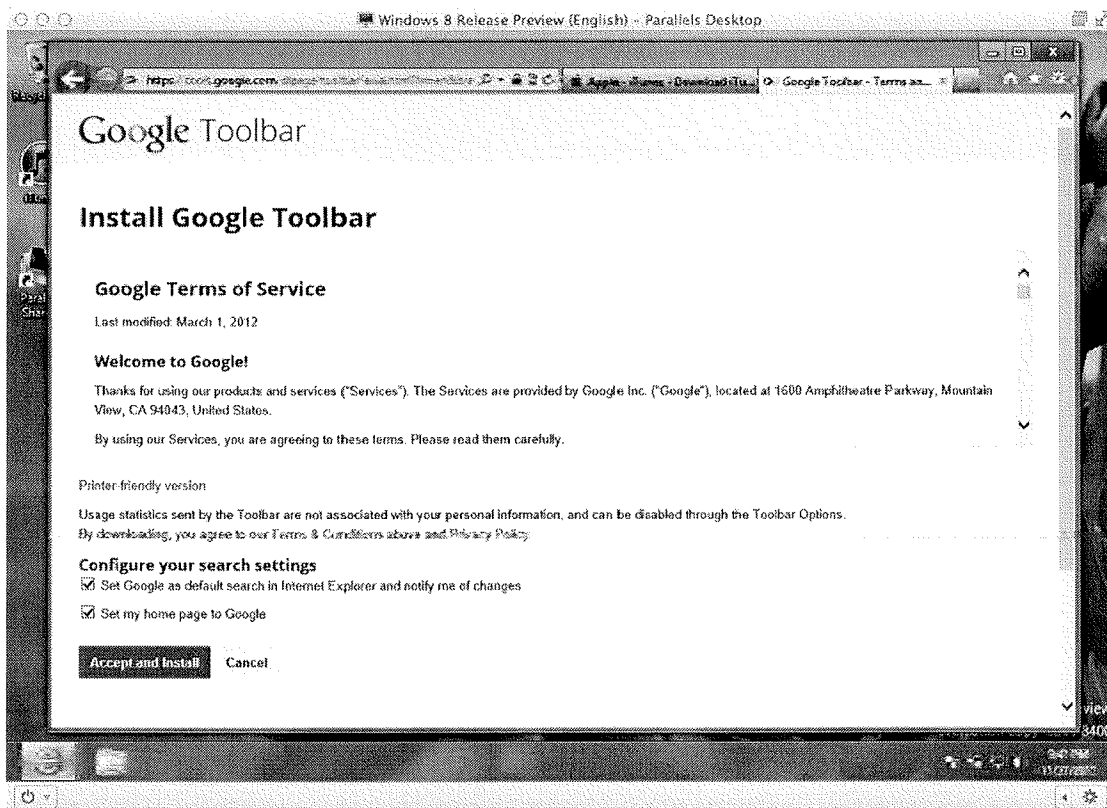


Image: Google Toolbar adds +1

1. **Headline:** Very clear.
 2. **Value Proposition Presented:** No.
 3. **Tracking Disclosed:** Not clearly. The language mentions that usage statistics will be sent, but they are not described and their uses are not mentioned.
 4. **All Essential Information Immediately Visible:** No, and all core terms within the Terms of Service are hidden beneath the fold.
 5. **Additional Legal Documents Immediately Accessible:** Yes.
 6. **No Bias Towards 'Accept':** No, as 'Accept and Install' is marketed with a significantly enhanced blue button background.
 7. **User Must Make an Active Decision:** Yes.
 8. **Decline is a Viable Option:** No, as the 'Accept and Install' option is the only option that will allow the installation to proceed.
- ii) Once the toolbar is installed, Google attempts to enable 'enhanced features.' This will include additional tracking and the linking of information collected with account the consumer has with other services operated by Google. Since Google operates many popular and highly personal services, like Gmail, Calendar, Drive, +1, YouTube, etc., the privacy implications of this change are potentially significant.

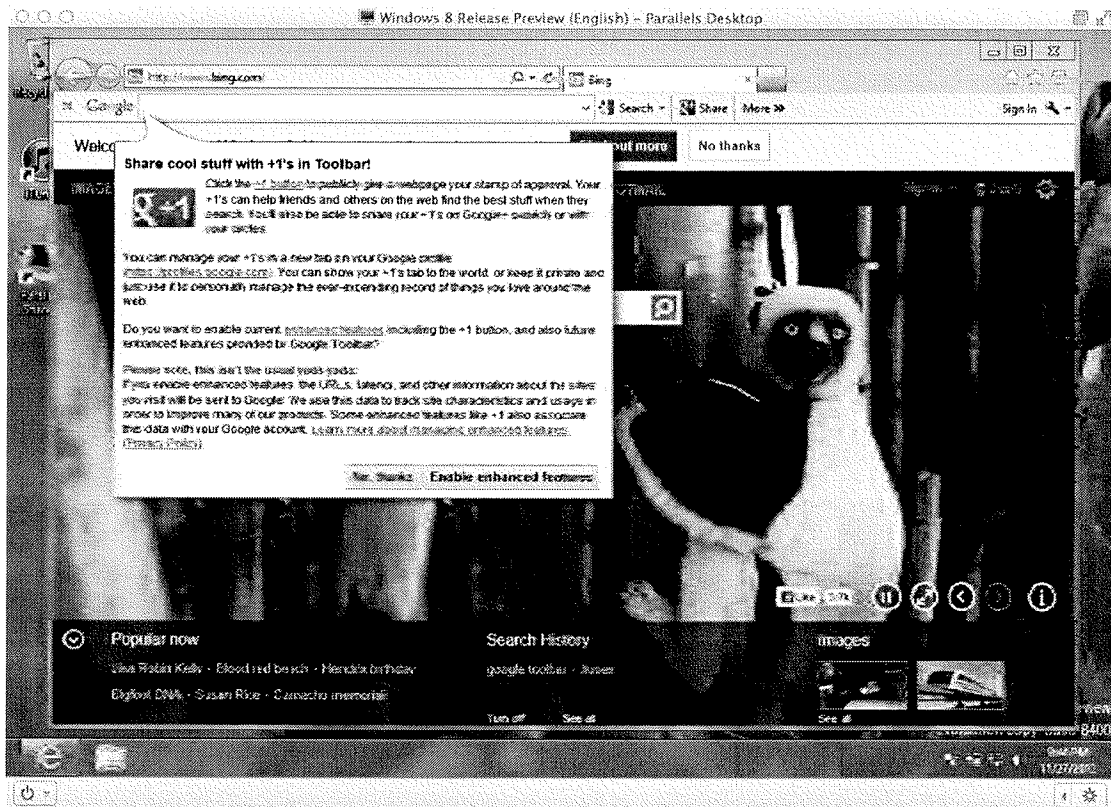


Image: Google Toolbar adds +1

1. **Headline:** No, as 'Share cool stuff ...' is clearly marketing oriented.
2. **Value Proposition Presented:** Yes.
3. **Tracking Disclosed:** Yes.
4. **All Essential Information Immediately Visible:** Yes.
5. **Additional Legal Documents Immediately Accessible:** Yes.
6. **No Bias Towards 'Accept':** Not entirely, as 'Enable ...' appears to be bolded to guide the consumer.
7. **User Must Make an Active Decision:** Yes.
8. **Decline is a Viable Option:** Yes.

APPENDIX A

Curriculum Vitae

Colin O'Malley

Chief Strategy Officer

Evidon, Inc.

28 West 44th Street, Suite 800

New York, New York 10036

(917) 262-2530

colin.omalley@gmail.com

Colin O'Malley is the Chief Strategy Officer for Evidon, Inc. In his current position, he works with companies to ensure their compliance with online privacy standards such as the Self-Regulatory Principles for Online Behavioral Advertising. Evidon's customers include WPP, Publicis, Dentsu, AmEx, Bank of America, Adobe, Procter & Gamble, and Ford. Prior to co-founding Evidon, he served on the executive team for TRUSTe, another leader in internet privacy. He is regularly sought after as a speaker and trainer regarding internet privacy issues.

Education

Vanderbilt University, 1995-1999

Bachelors of Science, Economics/Human and Organizational Development

Experience

Evidon, Inc., 2009-present

Chief Strategy Officer

Manages product strategy, including next generation ad technology executions and mobile implementations as well as policy outreach with regulators and trade associations like the IAB, DAA, MMA, and FTC, and across Europe. Recognized thought leader in the United States and European Union markets, authoring bylines for the trade publications and a frequent press referral. Oversaw embedding of privacy tags in advertisements that serve 2 billion times a day. Acquired and grew Ghostery, a browser extension with an opt-in panel of more than 7 million monthly users. Built long term relationships with many of the largest global agencies and brands (WPP, Publicis, Dentsu, American Express, Bank of America, Adobe, P&G, Ford, Walmart, Akamai).

TRUSTe, 2003-2009

Vice President of Strategic Partnerships and Programs

Spearheaded the rollout of commercial accreditation programs in web privacy, commercial email, downloadable software, and behavioral targeting markets. Carried revenue lines, managed P&L, built teams, and was a featured public face at industry events and government forums. Launched Trusted Download Program and Email Privacy Seal. Co-developed Bonded Sender Program.

Live Oak School, 2005-2008

Board Member

Served as a board member for a private, progressive K-8 day school with 230 students.

Vocab Vitamins, 2003-2007

Chief Executive Officer

Served as CEO for an online vocabulary service based on the classic word of the day mailing list concept with over 50,000 registered subscribers.

NetCreations, 1999-2002

Manager of Product Development

Managed product development at a permission email marketing firm that pioneered commercial applications of the double opt-in process. NetCreations was acquired by Return Path.

Publications

- 1) C. O'Malley, *ePrivacy – easy as one, two, three*, Fourth Source, September 7, 2012, available at <http://www.fourthsource.com/general/eprivacy-easy-as-one-two-three-10452>.
- 2) C. O'Malley, *EXPERT COMMENT: Evidon on the No-Nonsense Route to ePrivacy Compliance*, Strategy Eye, August 31, 2012, available at http://www.strategyeyedigitalmedia.com/article/2012/08/31/expert_comment_evidon_on_the_no-nonsense_route_to_eprivacy_co/.
- 3) C. O'Malley, *A Shorthand Guide to Compliance with the ePrivacy Directive*, admonsters, July 27, 2012, available at <http://www.admonsters.com/blog/shorthand-guide-compliance-eprivacy-directive>.
- 4) C. O'Malley, *The Pragmatist's Guide to Compliance with the ePrivacy Directive*, admonsters, June 27, 2012, available at <http://www.admonsters.com/blog/pragmatist%E2%80%99s-guide-compliance-eprivacy-directive>.
- 5) C. O'Malley, *How to Roll Out Cookie Consent*, iMedia Connection, June 12, 2012, available at <http://www.imediaconnection.com/content/32036.asp>.
- 6) C. O'Malley, *How to... Find Out Who's Tracking Your Website*, iMedia Connection, May 22, 2012, available at <http://www.imediaconnection.com/content/31819.asp>.
- 7) C. O'Malley, *EU e-Privacy Directive: Don't Call It a Cookie Law*, Econsultancy, May 16, 2012, available at <http://econsultancy.com/us/blog/9879-eu-e-privacy-directive-don-t-call-it-a-cookie-law>.
- 8) C. O'Malley, *The Difference Between Consent and Opt-in*, Association of Online Publishers, April 17, 2012, available at <http://www.ukaop.org.uk/news/eu-privacy-directive-consent-opt-in-cookies-evidon3549.html>.

- 9) C. O'Malley, *Understanding Tracking on Your Site*, iMedia Connection, April 3, 2012, available at <http://www.imediaconnection.com/content/31277.asp>.
- 10) C. O'Malley, *Why the Cookie Audit Rush?*, Association of Online Publishers, March 7, 2012, available at <http://www.ukaop.org.uk/news/how-to-run-a-cookie-audit3502.html>.
- 11) C. O'Malley, *Preparing for the EU Privacy Directive*, Association of Online Publishers, February 28, 2012, available at <http://www.ukaop.org.uk/news/eu-privacy-directive-publishers3403.html>.
- 12) C. O'Malley, *EU Privacy Directive—What's on the Slate for 2012*, Association of Online Publishers, March 15, 2012, available at <http://www.ukaop.org.uk/news/evidon-eu-privacy-directive-colin-omalley3277.html>.
- 13) C. O'Malley, *Cookie Law Update: Regulators Weigh In and Implied Consent Lives*, Chinwag, January 17, 2012, available at <http://chinwag.com/blogs/colin-omalley>.
- 14) C. O'Malley, *The Regulatory Crescendo in Europe*, Evidon Blog, December 21, 2011, available at <http://blog.evidon.com/2011/12/21/the-regulatory-crescendo-in-europe/>.
- 15) C. O'Malley, *The Privacy Icon Isn't an On/Off Switch*, Digiday, September 28, 2011, available at <http://www.digiday.com/platforms/the-privacy-icon-isnt-an-onoff-switch/>.
- 16) C. O'Malley, *Self-Regulation Solves the Do Not Track Problem*, IAB, February 23, 2011, available at <http://www.iab.net/iablog/2011/02/self-regulation-solves-the-do-.html>.

APPENDIX B

MATERIALS CONSIDERED

Complaint filed August 23, 2011 (Dkt. No. 1)
Answer filed December 13, 2011 (Dkt. No. 59)
Expert Report of Don Waldhalm dated September 17, 2012
RelevantKnowledge Privacy Policy and User Licensing Agreement, accessed Oct. 25, 2012, available at http://www.relevantknowledge.com/RKPrivacy.aspx
Sample Disclosure Dialog Boxes (Ex. A to comScore's Supplemental Response to Harris's First Set of Interrogatories)
Self-Regulatory Principles for Online Behavioral Advertising, available at http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf
Michael Learmonth, <i>Online Ad Industry Takes Aim at Microsoft in Congressional Hearing</i> , Ad Age Digital, June 28, 2012, available at http://adage.com/article/digital/daa-takes-aim-microsoft-congressional-hearing/235688/ .
Brad Berens, <i>FTC Chair Calls for Ad Transparency</i> , iMedia Connection, November 4, 2011, available at http://www.imediaconnection.com/article_full.aspx?id=30430
<i>White House, DOC and FTC Commend DAA's Self-regulatory Program to Protect Consumer Online Privacy</i> , PR Newswire, February 23, 2012, available at http://www.prnewswire.com/news-releases/white-house-doc-and-ftc-commend-daas-self-regulatory-program-to-protect-consumer-online-privacy-140170013.html
MP3 Cutter installation process, http://www.mp3-cutter-splitter.com/index.html .
Microsoft Silverlight installation process, http://www.microsoft.com/silverlight/
Adobe Reader installation process, http://get.adobe.com/reader/
Reuters webpage, uk.reuters.com
BBC webpage, http://www.bbc.co.uk/news/uk/
Chase Credit Card Application, https://applynow.chase.com/FlexAppWeb/renderApp.do?CELL=6H90&PROMO=DF01&SPID=DVW6
Nickelodean webpage, http://spongebob.nick.com/
Viacom Media Networks webpage, http://srp.viacom.com/sitefaq.html
Department of Homeland Security, Global Online Enrollment System webpage, https://goes-app.cbp.dhs.gov/main/goes
Safeway Club Card Application, http://www.safeway.com/CMS/includes/docs/Club_Card_App_SWY_052410.pdf
Install Google Toolbar webpage, https://tools.google.com/dlpage/toolbar/eula.html?hl=en&brand=GGHP&