Consultation Report: Race to the Bottom? 2007

LEGEND
Privacy-friendly and privacy enhancing
Generally privacy-aware but in need of improvement
Generally aware of privacy rights, but demonstrate some notable lapses
Serious lapses in privacy practices
Substantial and comprehensive privacy threats
Comprehensive consumer surveillance & entrenched hostility to privacy

Company	Company administrative details	Corporate Leadership	Data Collection and Processing	Data Retention	Openness and Transparency	Responsiveness	Ethical Compass	Customer Control	Fair Gateways	Privacy Enhancing or Invading Innovations	Initial Assessment	Justification
Amazon	Webform access to email for those with privacy problems. No postal address given. Must be signed in as an account holder in order to complain.	Previously profiled and shared profiles of customers' purchasing habits. Signed up to Safe Harbor.	Privacy notice describes some of processing practices. Does not discuss what is done with 'clickstream' and 'cookie data', i.e. whether Amazon tracks usage, popularity, and then profiles.	No information readily available	Policy lacking in information about how information is used to profile customers.		Previously Amazon has been reluctant to introduce privacy measures. Firm seems to have responded to earlier problems.	Customers may close accounts, but only possible through an email sent to Amazon.	Offers the choice to use anonymous or pseudonymous profiles and even informs customers of a variety of PET tools. Amazon Prime accounts offer greater services for an annual fee. Not mandatory and other customers are not penalised.	No privacy enhancing innovations apparent though points to privacy services from other companies. No discussions of techniques to profile.	Notable lapses	Amazon has improved much over the years but consumers should be informed on how their clicking, reading, and purchase habits are profiled and used.
AOL	Contact only available via email at *privacyquestions@aol.com* (though with a separate email address for Californians, at *CAPrivacyInfoAN@aol.com*.)		Tracks user movements and use of resources. Monitors which e-mails you open and act upon. Monitors searches and how these searches were acted upon. Keeps a track of history of items purchased across AOL services. Supplements data from other firms. Collects IP address and geographic information. Researches use of AOL services, using cookies and web beacons.	No information readily available	Policy is relatively open about the fact that there is personal information processing but is lacking in information about how.	Leakage of search engine data was responded to poorly as though it was not privacy invasive. Investigations showed otherwise.	Poor. Disclosed search data to U.S. Department of Justice for research purposes.	Closing account is possible but nothing is said about how long personal data is kept for aftewards.	Account-only access in many areas of site. Differentiates between different users (e.g. Apple users are prevented from viewing view video content).	No information readily available, though does use web beacons to track users activities.	Substantial Threat	No privacy enhancing innovations apparent though points to privacy services from other companies.
Apple	Apple Computer, 1 Infinite Loop, MS60-DR, Cupertino, California, USA, 95014 Privacy policy last updated in 2004. Numerous email addresses given based on geographic region including *privacy@apple.com* and *privacyeurope@apple.com*	Weak. Repeated statements in policy like: "As is true of most Web sites..." Relatively quiet on information processing issues. Member of Trust-e. Part of Safe Harbor.	Opt-out process available. Shares data with other companies to "manage and enhance customer data". Collects clickstream data. Does not consider IP address as personal information. Also collect 'clickthrough' data. Ministore collected list of music on home computers.	No specification of the deletion period. Does not consider itself responsible for data posted in forums, as a result is unlikely to anonymise or delete at any time.	Very little information is available. Vague privacy policy with an optimistic tone on data collection, but does not explain whether there is any profiling and marketing activities?	Kept quiet on the potential watermarking of DRM-free iTunes songs. They did respond eventually to the 'ministore' controversy. Subject access requests are said to be available according to the policy, by email.	Problematic. Sought to disclose the names of sources to bloggers' stories.	May opt-out of some services. May not access free iTunes services without registering.	Certain features of the Apple website will not be available once cookies are disabled.	Profiles use of music in 'Ministore'. Mentions privacy enhancing precautions, but no information on technologies. Uses cookies and "other technologies" to track users. Uses "pixel tags" to identify whether individuals have read emails.	Substantial Threat	Vague privacy policy does not address the advanced level of services offered by Apple. Could be quite promising if Apple was more open. Good that firm offers access to data subjects. Responsiveness has been poor to date.
BBC	Data Protection Officer, MC3 D1, Media Village, 201 Wood Lane, London, W12 7TQ and email at dpa.officer@bbc.co.uk		Use cookies to track movements. Uses Nielsen and SageMetrics cookies to track readership.	Declares in some cases how long personal information is kept.	Privacy policy is relatively explicit about each cookie, describing in detail.	No evidence yet. Charge 10 GBP for access to records.		Explains how to opt-out of cookies.		No information readily available	Generally privacy aware	Rare in its openness about processing, what for, and how to access data and manage cookies.
Bebo	Customer Support, Bebo, Inc.142 Tenth Street, San Francisco, CA 94103,USA	Co-operates with Child Online Exploitation Police in UK, after encountering problem cases.	Name, email address, IP address, age, hobbies, and interests and other content, such as photos. Does not consider IP addresses as personal information.	No information readily available	Inconsistencies in privacy policy. Lacks detail.	Responded to concerns about privacy problems (linked with child safety) but ensuring access is limited to certain age groups.		Can end membership. Can limit information available to people.	Company decides who can contact users based on their age.	No information readily available	Notable lapses.	Prior problems has led to some innovation. Lack of information is problematic. User control increasing.

Company	Company administrative details	Corporate Leadership	Data Collection and Processing	Data Retention	Openness and Transparency	Responsiveness	Ethical Compass	Customer Control	Fair Gateways	Privacy Enhancing or Invading Innovations	Initial Assessment	Justification
eBay	eBay Inc. Attn: Legal - Global Privacy Practices, 2145 Hamilton Avenue, San Jose, California 95125; and via a customer form	Member of Trust-e.	Information collection from other companies included.	No information readily available	Remarkable level of information about how data is shared.	Very responsive to privacy concerns: changed practice to allow for customer account deletion.		Can opt out of marketing and advertising. Can reject cookies though may have some effects.	Can gain access to much information without authenticating.	Uses web beacons. A lot of the cookies are only session cookies. Anonymised or de-identified information is shared.	Generally privacy aware	Good responsiveness. Web beacons and lack of information on retention detracts from score.
Facebook	156 University Avenue, Palo Alto, CA 94301; and *privacy@facebook.com*	Member of Trust-e. Signed up to safe harbor.	Earlier concerns about data matching, data mining and transfers to other companies. Collects data from 'other sources', including newspapers, blogs, instant messaging services, and other users of the Facebook service through the operation of the service (e.g. 'photo tags').	No information readily available	Basic privacy policy.	Has responded to some (of many) concerns about security and privacy.	Purports to have two principles: 1. you have control over personal information. 2. you have access to info others want to share. But track history indicates otherwise.	Unable to fully opt out of controversial 'news feed' services. Cookies can be blocked. Many are session cookies. Profiles are only accessible based on privacy settings, though name and profile-photo is available to all.	In 2005 a number of profiles were downloaded to prove weak security. Does not accept liability for security.	No information readily available	Substantial Threat	Problematic track history. Uses data from 'other sources', and has not maintained strong security mechanisms. Does not inform on measures being taken now to protect data.
Friendster	No specific privacy contact point. General address is given as Friendster, Inc. 568 Howard Street San Francisco, CA 94105 Fax: (415) 618-0074		Itemises information types collected through consent and without consent (e.g. IP address). Promises not to share personally identifiable information with third parties. Third party cookies are possible.	No information readily available	Open privacy policy, though vague at times.			User may chose to share with 'friends', 'friends of friends', and 'anyone', including non-Friendster members. Some profile information is shared with everyone.	Rejecting cookies may prevent access to website.	Access to personal information is said to be limited even to employees.	Notable lapses	Insufficient information to draw compelling conclusions. Lack of main point of contact is problematic.
Google	Privacy Matters, c/o Google Inc, 1600 Amphitheatre Parkway, Mountain View CA 94043 (USA). Policy not updated since 2005.	Rejected access to data by U.S. Justice Department for research purposes. Member of Safe Harbor.	Describes data collected. IP addresses are not considered personal information. They do not believe that they collect sensitive information. Do sometimes track links clicked upon. Shares information with consent, or to companies (subsidiaries, affiliated companies, trusted businesses or persons).	Unclear but has stated 18-24 months as eventual outcome. Log history is retained after this period.	Vague, incomplete and possibly deceptive privacy policy. Document fails to explain detailed data processing elements or information flows.	Generally poor track record of responding to customer complaints. Ambivalent attitude to privacy challenges (for example, complaints to EU privacy regulators over Gmail).	Privacy mandate is not embedded throughout the company. Techniques and technologies frequently rolled out without adequate public consultation (e.g. Street level view).	Customers have a right to amend personal details held by Google but does not allow search history to be removed. Most services do not permit user access to specific or aggregated disclosure or tracking data.	Opt-out possible for some services. Some services may not work well without cookies. May access essential resources without account but when account is created it is sticky.	Will utilise Doubleclick's "Dynamic Advertising Reporting & Targeting" (DART) advanced profiling system.	Hostile to Privacy	Track history of ignoring privacy concerns. Every corporate announcement involves some new practice involving surveillance. Privacy officer tries to reach out but no indication that this has any effect on product and service design or delivery.
Hi5	General Counsel, hi5 Networks, Inc., 455 Market St., Suite 910, San Francisco, CA 94105,USA.		Collects gender, date of birth, and ZIP. Track users with cookies and by IP addresses. Also tracks users movements on site by monitoring click-through data.	No information readily available	Relatively blatant about some processing but unnecessarily vague about others.		Poor. Clicking on Privacy Policy opens up a pop-up window advertisement!	User can identify what information is available to members vs. non-members. Can view other users' profiles without notifying that user. Can opt-out of receiving some information. May delete account.	All visitors can see public content on server (do not need to be registered).	No information readily available	Substantial Threat	Preposterous use of advertising technique (pop-up window) when clicking on privacy policy. Point of contact being a General Counsel leaves little confidence is responsiveness.

Company	Company administrative details	Corporate Leadership	Data Collection and Processing	Data Retention	Openness and Transparency	Responsiveness	Ethical Compass	Customer Control	Fair Gateways	Privacy Enhancing or Invading Innovations	Initial Assessment	Justification
Last.fm	No contact information given for specific access on privacy, though user is suggested to use 'feedback page'.		Email address is not required to register. Pseudonymous listening habit data will be available to other users. May sell or licence lists, but not personal data. No personal information collected regarding transactions with third sites. Monitors which songs listened to, whether skipped, etc., recommendations to other users Does not process PII relating to record collection Does not collect ZIP, post code, city or country unless user explicitly shares. Regards IP addresses as anonymous.	No information readily available	Thorough privacy policy.			Appear to be willing to issue a new user name or password if account anonymity has been destroyed.	Can identify users and what they are listening to without authenticating. Session cookies only. Turning off cookies will inhibit 'a significant proportion' of access.	Appears to collect only aggregate data when possible.	Generally privacy aware	More openness on how to appeal would help case. Explicit use of anonymised data is promising, though more detail on how this is done technologically would increase confidence.
LinkedIn	LinkedIn Corporation, Attn: Privacy Policy Issues, 2029 Stierlin Court, Mountain View, CA 94043 or privacy@linkedin.com	Members of Trust-e and Safe Harbor.	Claim that email addresses of friends that user includes are only used for inviting those friends, and sending reminders. Use cookies and web beacons. Permits third-party cookies and beacons. Shares information with other companies "for specific services".	May close account and then data may be deleted (but not necessarily).	Privacy policy outlines some situations where information is used but could be more explicit.			Some level of user control over information, e.g. friends' information is not accessible to others without permission. Can opt-out of public profile. May close account but only via email.	Users within three degrees of a network can see profile information. Only direct connections can see email address. Public profile is viewable by non-users.	"Any sensitive information that you provide will be secured with all industry standard protocols and technology" Use web beacons to profile and advertise by general profile, e.g. business managers in Texas.	Notable lapses	Use of email addresses of non-users and beacons is questionable. Accessibility of personal profiles could be better managed. Can close account but only via email.
LiveJournal	privacy@livejournal.com		Describes how and why information is collected, including IP addresses. IP addresses may be given to other journal owners within LiveJournal. However IP addresses are not considered sensitive for marketing.	Allows account closure, though keeps some information.	Clear and simple privacy policy. Have a procedure for data security breaches.			Account closure is possible.		Uses "physical, electronic, and procedural safeguards".	Generally privacy aware	More clarity about privacy enhancing innovations is needed. Lax attitude towards IP addresses is problematic. Good to have procedure on data breaches.
Microsoft	Microsoft Privacy, Microsoft Corporation One Microsoft Way Redmond, WA 98052	Established elaborate privacy reporting and awareness regime throughout the company. Developed the "laws of identity". Member of Safe Harbour and Trust-e.	May combine personal information derived from a spectrum of MS services. Shares information to partners (subsidiaries, affiliated companies, trusted businesses or persons). Permits third party advertisers to deploy cookies.	No information readily available	Lacks adequate detail of retention periods, data flows and targeting techniques. When pushed, has been open about some privacy problems.	Improved level of responsiveness to privacy concerns and customer feedback, though continues to be dominated by a PR imperative.	Privacy has now been embedded throughout all stages of the design process for MS products, though patchy management, oversight and reporting results in notable failures such as WGA.	Easily accessible and navigable account management pages. Little information available on accessing or deleting hidden data (logs etc).	MS Passport is used across services, though not required for some services and level of 'stickiness' is insufficiently tested.	Extremely poor privacy design of Windows Genuine Advantage (WGA) and Passport. Strong privacy design and principles in CardSpace.	Serious Lapses	More information on retention is required. Policy is too basic despite application to a number of services. Have embedded privacy into many product and service designs, but terrible track record, including recent WGA debacle.

Company	Company administrative details	Corporate Leadership	Data Collection and Processing	Data Retention	Openness and Transparency	Responsiveness	Ethical Compass	Customer Control	Fair Gateways	Privacy Enhancing or Invading Innovations	Initial Assessment	Justification
Myspace	8391 Beverly Blvd, #349, Los Angeles, CA 90048, privacy@myspace.com		Explicit in collecting name, email address, and age; other profile data including but not limited to: personal interests, gender, age, education and occupation. Considers IP addresses as non-identifying information, to track usage, and to share with third parties. Data is recorded for security and monitoring purposes. May opt-out of receiving service information. Email addresses are kept, particularly for invitations, though recipients of invitations can contact myspace to have email address removed. Allow cookies and third party cookies.	No information readily available		Public profiles are no longer mandatory.	Tried to require subpeonas before handing over information to law enforcement authorities (on suspected sex offenders).	Users may block the receiving of myspace invitations by emailing myspace with a subjet 'block'.	Email addresses and user names are limited in their disclosure.	No information readily available	Notable lapses	A mixed bag, with some strong protections and a lot of ambiguities. Problematic interpretation of IP addressing data. Invitation recipients can opt-out. Account deletion is unclear.
Orkut	Privacy Matters , c/o Google Inc. 1600 Amphitheatre Parkway, Mountain View CA 94043 (USA)		Must have a Google Account, including email address. Possible profile information: gender, age, occupation, hobbies, and interests, plus other content, such as photos	Can delete account, completed within 48 hours. Retain contents of messages for indeterminate amount of time.	Very limited privacy policy.		Ethical challenges in blocking site from access in Iran.	Invitees can choose to not receive invites.	Must have a Google Account.	No information readily available	Serious Lapses	No Orkut-specific privacy contact information. Limited privacy policy. Account deletion good sign. Checkered history in co-operating with governments. Requires registration to view information, but registration applies across Google services.
Reunion.com	Reunion.com, Inc., Attn: Privacy Policy Officer, 2118 Wilshire Blvd. Box 1008, Santa Monica, CA 90403-5784		Collects at a minimum, name, birth date, gender, email address and zip code Uses real names. Company will contact users. May "engage third parties to perform analysis or data processing of our databases that involves access to this information in order to better provide you with the services for which you joined" Shares information with other sites. Tracks movements on site and with partner sites.	No information readily available	Changes to policy are announced but if user continues to use site, they have consented to the changes. May transfer information if firm is purchased.		Poor. Admonished by businesses community for misleading advertising practices to bring in new registrants.		Not accepting cookies will limit access.	Does protect email privacy through a relay system. Use 'technical, administrative and physical safeguards" to protect security of personal information.	Substantial Threat	Promising for use of email relaying. Data sharing is dangerously vague. Tracking usage is problematic. Historical ethics problems.

Company	Company administrative details	Corporate Leadership	Data Collection and Processing	Data Retention	Openness and Transparency	Responsiveness	Ethical Compass	Customer Control	Fair Gateways	Privacy Enhancing or Invading Innovations	Initial Assessment	Justification
Skype	15, rue Notre Dame, L-2240 Luxembourg, Luxembourg and/or Skype Communications S.A though no explicit address given for privacy concerns.		Registration not required. Invitation email addresses are deleted immediately upon sending invitation. No communications from skype other than messages about faults. Shared with third parties for provision of services. Cookies do not contain identifying information. Third party cookies exist.	Vague. At least deals with the issue in part in the privacy policy without committing in detail. Though for traffic data, commits to "erase Traffic Data, or make Traffic Data anonymous, as soon as it is no longer needed for the purpose of the transmission of the communication or for billing purposes, unless applicable law permit otherwise."	No way to know if there are back doors in the software. Right to review data, correct, and delete personal data, via email delete@skype.com Thorough privacy policy, but no contact information for accountability.	Responded to concerns about DRM and reading motherboard information.	Poor. Co-operated with Chinese government.		Do not need to register to use Skype Software, but registration may be needed for particular services. Blocking cookies may inhibit personalised services.	User profile data not stored centrally on server. Takes 'appropriate organizational and technical measures'; authorised employees only. Will take "appropriate technical measures to protect the confidentiality of the Communications Content via its Skype Software and VoIP Services"	Notable lapses	Good promises on deleting invitation email addresses. Lack of contact details is problematic. Lack of openness about software capabilities is problematic. Deletion of traffic data is good statement though less ambiguity about role of laws would help.
Wikipedia	No explicit contact, but policy says it was approved by Board.		Can operate under pseudonym, but if not, then logs IP addresses for public view. Recommends using pseudonym. IP addresses are stored and can be seen by server administrators and advanced users. Data is combined to investigate abuse.	Raw logs are normally discarded after two weeks. Unable to remove accounts. Deleted 'content' is not in fact deleted.	Clear privacy policy, but no main point of contact.				Fully accessible without authenticating.	Session cookies only, and temporary log-in cookies that expire every 30 days.	Generally privacy aware	Lacking in some information, such as contact details. Good statement on retention policy, though unless there is a contact, this is unverifiable.
Windows Live Space	Microsoft Privacy, Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052 · 425-882-8080, and webform is available.	Signed up to Trust-e and Safe Harbor.	IP addresses not treated as personal information. Customised links are used to identify users. Voice messenger service requires signing up with Verizon. Tracks all requests for maps. Locations are logged when service is used online.	No information readily available	Unclear about what information is used for and how long it is used for.		Poor. Co-operated with Chinese government. Unclear policy statement about future co-operation. Recent research hints at profiling based on search requests. Disclosed search data to U.S. Department of Justice for research purposes.	User can designate who has access to which calendar data.	Anyone may review calendar information that is published for public access.	May use beacons to track messages sent by MS to determine whether opened or read. Beacons also used by third parties to aggregate statistics.	Substantial Threat	Problematic use of personal information, without clear statements about retention. Uses almost every means to identify users and track movements.
Xanga	Contactable through webform for email interaction.		Username, password, email address, date of birth. Email and birthdate are not necessarily disclosed if user wishes. Profile information is optional. For invitations, Xanga may send multiple invitations by email. Email addresses can be blacklisted to receive no further invitations. Logs IP data. Targets advertisements based on profile and past activities. Third party cookies are possible as well. May transfer data if company is purchased.	If account is shut down, Xanga site no longer accessible. Data may be archived, but offline.	Presumes consent by non-U.S. users.			By default information is shared widely, though can be controlled. Can control comments on your section of the site, and whether someone can be blocked from commenting.	Information available to non-registered users. Blocking cookies may limit access.	Footprints' service allow users to watch visitors on his or her own site (username or geographic information based on IP address).	Serious Lapses	Invitation process could be better managed. Treatment of IP data is vague. Profiling is mentioned but more clarity is required. Information should not be shared by default. May limit information collected.

Company	Company administrative details	Corporate Leadership	Data Collection and Processing	Data Retention	Openness and Transparency	Responsiveness	Ethical Compass	Customer Control	Fair Gateways	Privacy Enhancing or Invading Innovations	Initial Assessment	Justification
Yahoo!	Yahoo! Inc. Customer Care - Privacy Policy Issues, 701 First Avenue, Sunnyvale, CA 94089, (408) 349-5070	Trust-e and safe harbor.	Registration process can be combined with data from other sources (business partners and other companies). Information collected: name, email, birthdate, gender, ZIP code, occupation, industry, personal interests. May also ask for social security for financial services. Collects transaction data, including information about use of financial products. Collects and stores information including IP addresses and cookies related data. Data can be shared for marketing purposes. Data will be transferred if acquired. Cookies (and third party cookies) are used, as are web beacons. Opt-out of marketing information.	May delete account but some information retained, for 90 days. Log files are used — after they are used they are stored (but said to be inaccessible). No further information on searches.	Overly broad and vague policy.	Did not go out of its way to respond to ethical concerns.	Poor. Cooperates with governments with disclosure of information, including Chinese government. Disclosed search data to U.S. Department of Justice for research purposes.		Registration not necessary for some services.	Use 'physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information' Also limit access to employees.	Substantial Threat	Vague privacy policy prevents us from understanding the dynamics of data processing. Using information from other sources is highly problematic. Account closure possibility is good (and honest statement about retention is relatively positive). Lack of information on search and IP data is problematic. Poor track record.
YouTube	Contact only available through a contact form.		Video, image, or other content posted are not considered personal information. Use both session and persistent cookies, as well as web beacons. Monitors and tracks IP logs. IP data not considered personal data. Data used to monitor marketing effectiveness and track actions (e.g. entries). Share personal information with subsidiaries, affiliated companies, or other businesses and persons.	Media files, once uploaded, can not be modified. No information on deletion of other data.	Use of site is considered consent to U.S. law (no safe harbor). Data can be purchased in event of sale.	Has a policy for data breaches.			Blocked cookies may inhibit service.	Web beacons used to track usage, and uses gifs in emails to track users. "[U]ses commercially reasonable physical, managerial, and technical safeguards to preserve the integrity and security of your personal information"	Serious Lapses	Considering the size of YouTube and its owners, the vague information about sharing of personal information with affiliated companies leaves much to be desired. Tracking email reading habits is problematic. Videos are not considered personal information. Explicit statement that 'consent' is presumed in transborder data flows is questionable.