PRIVACY INTERNATIONAL

A Race to the Bottom – Privacy Ranking of Internet Service Companies

Archived report by Privacy International
June 2007

PRIVACY INTERNATIONAL

Table of contents

A consultation report

This report has been prepared by Privacy International following a six-month investigation into the privacy practices of key Internet based companies. The ranking lists the best and the worst performers both in Web 1.0 and Web 2.0 across the full spectrum of search, email, e-commerce and social networking sites.

The analysis employs a methodology comprising around twenty core parameters. We rank the major Internet players but we also discuss examples of best and worst privacy practice among smaller companies.

The report was compiled using data derived from public sources (newspaper articles, blog entries, submissions to government inquiries, privacy policies etc), information provided by present and former company staff, technical analysis and interviews with company representatives.

Because the 2007 rankings are a precedent, Privacy International will regard the current report as a consultation report and will establish a broad outreach for two months to ensure that any new and relevant information is taken into account before publishing a full report in September.

Interim results are available here in PDF format: Interim Rankings

About Privacy International

Privacy International (PI) was established in 1990 as a human rights research and campaign organization. It was the first privacy NGO to operate in the global environment and since then has been instrumental in the evolution of the modern international privacy movement. Its key functions are to provide technology assessment, develop reviews of public policy and to act as a watchdog on surveillance by governments and corporations. PI is based in London, and has an office in Washington, D.C. Together with members in 40 countries, PI has conducted campaigns throughout the world on issues ranging from wiretapping and national security activities, to ID cards, video surveillance, data matching, police information systems and medical privacy, and works with a wide range of NGO's, academic institutions and inter-governmental organizations. PI's primary source of funding comes from philanthropic and charitable organizations.

We have previously led campaigns and taken action against the practices of a number of companies including:

- Campaigning against corporate privacy practices, e.g. Amazon
- Identifying the problems in technology design, e.g.problems with advertising in Gmail
- Monitoring and campaigning against the disclosure of data from companies to governments, e.g. EU-US PNR, SWIFT, Telecommunications companies
- Founding and running the Big Brother Awards, now held annually in over 15 countries, that identify 'worst corporate invaders'
- Campaigning against bad practice in account management, for instance preventing users from deleting accounts, e.g. against Amazon and eBay
- Ranking countries for their privacy protection and surveillance levels.

Building particularly from our work on companies' practices on customer account management and our expertise developed in the country rankings we are now positioned to develop rankings for companies.

Why have we undertaken this study?

For many years, consumers and companies have approached Privacy International asking for our suggestions of good company practice in privacy protection. In the past this has been difficult for us to achieve for a number of reasons, including:

- Privacy International does not endorse specific companies
- We know the dynamics of this field well enough to understand that even if a company exhibits good privacy practice today, it can quickly change those practices for the worse by tomorrow
- It is very difficult and time consuming to accurately discover the privacy practices of a given company and it is often the case that these companies are not fully aware of their own information handling procedures.

We are increasingly concerned about the recent dynamics in the marketplace. While a number of companies have demonstrated integrity in handling personal information (and we have been surprised by the number of 'social networking' sites which are taking some of these issues quite seriously), we are witnessing an increased 'race to the bottom' in corporate surveillance of customers. Some companies are leading the charge through abusive and invasive profiling of their customers' data. This trend is seen by even the most privacy friendly companies as creating competitive disadvantage to those who do not follow that trend, and in some cases to find new and more innovative ways to become even more surveillance-intensive.

We felt that consumers want to know about these surveillance practices so that they can make a better-informed decision about how, whether and with whom they should share their personal information. We also believe that companies need to be more open about how they process information and why it is processed.

Most importantly, we wanted to indicate to the marketplace that their surveillance and tracking activities are being scrutinised.

Background

PI has tracked the development of the Internet since the creation of the World Wide Web in the early 1990s. We have continually voiced our concern that this medium provides the potential for a haemorrhage of personal privacy, and we have argued for some years that Internet companies should embrace a wider range of privacy protections for users.

The privacy threat on the Internet arises from a number of factors. Increasing disclosure by consumers of personal information allows companies to capture and process data to a significant extent. New technologies permit the capture of increasingly detailed levels of information. Meanwhile, new Internet products often involve a requirement for user registration, enabling of identifying techniques and agreement to terms and conditions that are frequently hostile to privacy.

However the emergence over the past three years of an aggressive move by major Internet companies into "ad space" has created the most recent and possibly most dangerous threat to privacy. With the creation of a greater range of products and services, increased disclosure of personal information and the evolution of a huge user population came the opportunity to establish new forms of user targeting and profiling to generate greater advertising revenue.

Privacy International has been concerned that this development may result in a "lowest common denominator" for privacy. In contrast to the 1990's vision of the Internet, in which strong privacy could become a market differentiator, the reality in 2007 is that all major Internet players may move to establish a level of user surveillance that results in little or no choice for Internet users and relatively few meaningful privacy mechanisms. Market domination by a handful of key players will ensure that without care, a race to the bottom will evolve during the immediate future.

Our decision to undertake the privacy ranking study is a first attempt at understanding the full spectrum of the privacy threat and to discover where each key player stands with regard to privacy protection. The long term goal of this report is not necessarily to "name and shame" but to highlight crucial trends and imperatives that will shape the future of privacy on the Internet.

A consultation report

This is a consultation report for the following reasons:

- While the data used for this analysis provides a very strong indication of privacy practices, we wish to reach out for more data on how companies' process information. Too many companies presume that statements framed in legal language within their privacy policies actually describe their true information collection and processing practices. When our legal experts reviewed a spectrum of privacy policies we became alarmed at how much we still do not know. We felt that additional time should be allocated in the hope that companies will come forward with more data. The fact that we, as specialists in this field, cannot fully understand the full range of surveillance practices of some companies leaves us greatly concerned about the ability of consumers to make informed decisions in the marketplace.
- We are soliciting comments on the findings of this report from companies, consumer organisations, industry associations and other experts on practices and additional elements. We have been in touch with a number of the companies involved in this study and we hope to receive further relevant information. If useful information is not offered we will wherever possible use legal mechanisms to obtain it.
- We are seeking the assistance of regulators who might help illuminate some of the more arcane collection and processing practices. Privacy commissioners from around the world and even the U.S. Federal Trade Commission can, we hope, help us uncover some of legal challenges arising from the data processing practices of these companies.

A more detailed report will be available in September.

Which companies?

Ideally we would like to be able to look at all companies in all sectors, but for now we have limited ourselves to online service companies. We created a list of consumer-facing companies based on a number of 'top 50', 'top 100', and 'top 500' resources using criteria including:

- market share
- services offered
- number of users
- site traffic

We have solicited comments from experts around the world about companies that we may have unintentionally omitted. For the time being we have excluded coverage of companies operating under mandatory data collection regimes such as those in the financial sector (e.g. online banking and payment schemes) and the travel industry (e.g. airlines and travel agencies).

Categorising companies has become increasingly difficult. The amount of mergers and acquisitions sometimes makes it quite difficult to differentiate stand-alone companies from conglomerates. We had to judge when it was appropriate to differentiate between companies and services. For instance, Windows Live Space is part of Microsoft, but because it offers services that are quite specific and because of the size of the user base, we took the decision to treat it as a distinct organisation. Meanwhile, Google is a company comprising many services, but its practices and ethics are very much part of its brand and image as a whole, and so we treated it as one single entity. We ranked Orkut as a separate entity even though it is owned by Google.

We are open to recommendations for other companies that we should include in future ranking reports. Ideally we should be able to segment the report findings into various sectors. For instance, we could identify the best and worst practices within social networking sites, search engines and location-based services. We are looking into expanding our company list in the future, but we must also conduct research and consult widely on how looking at specific service dynamics will affect the methodology. It should also be noted that due to resource constraints many of the companies on our current list operate predominately in the English language. We hope to broaden the language base in future rankings. Due to these constraints we have currently omitted some of the largest companies on the Internet.

The companies we included in this consultation study are:

- Amazon
- AOL
- Apple
- BBC
- Bebo
- eBay
- Facebook
- Friendster
- Google
- Hi5
- Last.fm
- LinkedIn
- LiveJournal
- Microsoft
- Myspace
- Orkut
- Reunion.com
- Skype
- Wikipedia
- Windows Live Space
- Xanga
- Yahoo!
- YouTube

We also reviewed the practices of other companies that are not necessarily market leaders. Through investigation and research, sometimes spurred by communications we receive from concerned members of the public, we identified a number of smaller companies who sometimes exercise a complete disregard for the sensitivity of their customers' personal information.

We are also searching for companies that exhibit positive privacy practices. We have been able to identify a number of these companies and hope to report on them more fully in our September report.

Methodology

In wide consultation with experts from around the world we were able to identify the following ranking categories for analysis:

Corporate administrative details

Does the company actually have a department or individual responsible for privacy compliance? The policy will have limited effect if users cannot question the processing of personal information. Some companies have designated privacy officials or embed privacy protection within the legal branch of the firm, while others do not even publish contact information.

Corporate leadership

Assesses whether a company plays a strong public role in protecting and promoting privacy in the marketplace (this must be matched with authority and action, not just mere words), or whether the firm is a leader in the trend toward profiling, sharing and disclosure of customer data. We also looked into whether the company is using industry-recognised self-regulatory mechanisms (e.g. Trust-e) and whether the company has signed up for the Safe Harbor agreement between the EU and the U.S.

Data collection and processing

What type of information does the site collect, with and without consent? On some sites the personal information submitted by customers is necessary (e.g. billing addresses) but there are many sites that collect information that may be unnecessary (age, marital status, home address, preferences, medical information, extraneous financial information) from customers without adequate information about why this information is needed and how it is used. Some companies may collect and mine other information, such as viewing habits and preferences (e.g. musical genre, lifestyle choices etc.)

Here, it is also important to note the status of 'Internet Protocol Addresses' (IP addresses). Many companies state that they see this data as non-personal – even anonymous – information, permitting them to collect and track users' movements around the site to determine what a specific user reads. This approach permits profiling of a user's habits and interests.

Data retention

Some companies delete the information they collect once it is no longer needed. Other companies are not quite so clear, and a few sites are quite open that they do not intend to delete personal information at all (or at least not until they are ready to do so). With increased consumer concern about information breaches from stolen and lost computing resources, or through malicious hackers gaining access to resources, companies need to be aware that the risk to their market position and customer base may be proportionate to the amount of personal data they store.

Openness and Transparency

It is fair to say that most organisations have now created privacy policies. These privacy policies often say much but disclose relatively little about a company's true practices. Some companies also cover up or refuse to engage publicly about privacy concerns. Here we rate these companies on how open they are to the public about their actual practices. We look at their privacy policies to assess whether they are merely a collection of disarming words (that usually starts with 'At [company X] we take your privacy seriously') with little detail, or which even highlight contradictory practices.

Disappointingly, many of the privacy policies seem to have been written with the same goal: to say very little but in as complex a way as possible. Yet there are also some policies that are exemplary in their eloquence and detail, describing every element of information and how it is processed by the company.

Responsiveness

Disarming statements about privacy do little to compensate for the lack of responsiveness to consumers who have privacy concerns. We are in a continuing process of contacting companies to see how they respond to privacy queries and concerns and whether those concerns are dismissed (as we have seen in some remarkable situations where in one case a company told us 'Life is too short (to worry about privacy)' or obfuscated (where companies respond with platitudes but disclose very little).

We look back over the history of the company to see how they responded to privacy problems and when those were brought to their attention, to measure the sincerity of these companies in protecting their customers' information. We also assess whether a company allows users to access and correct their personal information through 'subject access requests' or similar mechanisms.

Ethical compass

Have these companies encountered ethical challenges and how have they dealt with them? Have they co-operated with problematic warrants and access contentious requests from law enforcement agencies and foreign governments? How have they responded to customers' concerns? These actions go some way to explaining how seriously a company treats their customers' personal information.

Customer and user control

In our earlier research and campaigns we identified a number of companies that were unwilling to let customers delete their accounts. This widespread practice is not only problematic for privacy (in that your data can never be deleted) but also calls into question whether companies are properly marketing themselves as 'x million customers' when in fact there are only 'x thousand' active customers.

User control in the age of advanced customer activity (such as in social networking sites) should also allow customers the ability to control who has access to personal information, whether this access can be limited and even, when possible, when it should be anonymized. There has been a remarkable level of activity in this area since the security concerns over social networking emerged and we are optimistic that new protections will emerge.

Additionally, we assess whether customers can choose for themselves what types of information they disclose.

Fair gateways and authentication

Online services increasingly require individuals to create accounts in order to gain access to services, whether to look at itineraries, read articles or conduct searches. Sometimes these access controls are privacy enhancing, where they can aid individual consumers in preventing the trawling of their personal profiles by unwelcome visitors. However we are concerned at the increased profiling of customers' preferences based on the resources companies gain access to (e.g. profiling individuals based on the material they read). We have also taken into account scenarios where a decision to block any form of surveillance may intefere with the resulting level and quality of service.

Privacy enhancing innovations and Privacy invasive innovations

Some companies have implemented advanced techniques to protect privacy through advanced use of encryption (beyond simple SSL) and identity management technologies, amongst others. But 'innovation' need not only be technology-based, but could also reflect advanced and progressive attitudes toward information processing, such as promoting the use of pseudonymous accounts. We highlight these practices where such information is available.

Conversely, many companies are investing vast amounts of funds into privacy invasive practices, and most hope to be the first to market these innovations. We highlight when companies use blunt instruments to collect personal information without consent, and when they use pinpoint precision to delve deeper into personal profiles. While many companies use cookies (in a variety of ways) a number of companies go well beyond this practice into using 'web beacons' or 'pixel tags' to even identify whether users are reading their emails.

Analysis

Where possible we present data on specific privacy practices. It was not always possible to precisely assess a company's approach in each category. As a result, we erred on the side of caution and gave the company the benefit of the doubt and assessed it only for what we could actually identify.

We look forward to working with the relevant companies in the coming months to complete the study – this will be expanded in the September report. We look forward to receiving compelling evidence that a given company respects the privacy of its users, and protects their personal information accordingly.

We will also be reaching out to even more experts from around the world who may recommend additional categories and even other companies to include in this study.

As a result, some findings of this report may change substantively.

Each category is currently assessed based on a color-band system:

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

Companies were given a rating for each category and the average results (in categories where there was data) resulted in the final assessment. So while many of the companies demonstrated both positive and detracting features, we calculated an average score.

This result was then double-tested by presenting experts with the qualitative findings without any category-level assessment and we asked for the experts' own assessments. The convergence of all our assessments is provided as 'initial findings'.

Results are available here in PDF format: Interim Rankings

Why Google?

We are aware that the decision to place Google at the bottom of the ranking is likely to be controversial, but throughout our research we have found numerous deficiencies and hostilities in Google's approach to privacy that go well beyond those of other organizations. While a number of companies share some of these negative elements, none comes close to achieving status as an endemic threat to privacy. This is in part due to the diversity and specificity of Google's product range and the ability of the company to share extracted data between these tools, and in part it is due to Google's market dominance and the sheer size of its user base. Google's status in the ranking is also due to its aggressive use of invasive or potentially invasive technologies and techniques.

The view that Google "opens up" information through a range of attractive and advanced tools does not exempt the company from demonstrating responsible leadership in privacy. Google's increasing ability to deep-drill into the minutiae of a user's life and lifestyle choices must in our view be coupled with well defined and mature user controls and an equally mature privacy outlook. Neither of these elements has been demonstrated. Rather, we have witnessed an attitude to privacy within Google that at its most blatant is hostile, and at its most benign is ambivalent. These dynamics do not pervade other major players such as Microsoft or eBay, both of which have made notable improvements to the corporate ethos on privacy issues.

In the closing days of our research we received a copy of supplemental material relating to a complaint to the Federal Trade Commission concerning the pending merger between Google and DoubleClick. This material, submitted by the Electronic Privacy Information Center (EPIC) and coupled with a submission to the FTC from the New York State Consumer Protection Board, provided additional weight for our assessment that Google has created the most onerous privacy environment on the Internet. The Board expressed concern that these profiles expose consumers to the risk of disclosure of their data to third-parties, as well as public disclosure as evidence in litigation or through data breaches. The EPIC submission set out a detailed analysis of Google's existing data practices, most of which fell well short of the standard that consumers might expect. During the course of our research the Article 29 Working Group of European privacy regulators also expressed concern at the scale of Google's activities, and requested detailed information from the company.

In summary, Google's specific privacy failures include, but are by no means limited to:

- Google account holders that regularly use even a few of Google's services must accept that the company retains a large quantity of information about that user, often for an unstated or indefinite length of time, without clear limitation on subsequent use or disclosure, and without an opportunity to delete or withdraw personal data even if the user wishes to terminate the service.
- Google maintains records of all search strings and the associated IP-addresses and time stamps for at least 18 to 24 months and does not provide users with an expungement option. While it is true that many US based companies have not yet established a time frame for retention, there is a prevailing view amongst privacy experts that 18 to 24 months is unacceptable, and possibly unlawful in many parts of the world.
- Google has access to additional personal information, including hobbies, employment, address, and phone number, contained within user profiles in Orkut. Google often maintains these records even after a user has deleted his profile or removed information from Orkut.
- Google collects all search results entered through Google Toolbar and identifies all Google Toolbar users with a unique cookie that allows Google to track the user's web movement.17 Google does not indicate how long the information collected through Google Toolbar is retained, nor does it offer users a data expungement option in connection with the service.
- Google fails to follow generally accepted privacy practices such as the OECD Privacy Guidelines and elements of EU data protection law. As detailed in the EPIC complaint, Google also fails to adopted additional privacy provisions with respect to specific Google services.
- Google logs search queries in a manner that makes them personally identifiable but fails to provide users with the ability to edit or otherwise expunge records of their previous searches.
- Google fails to give users access to log information generated through their interaction with Google Maps, Google Video, Google Talk, Google Reader, Blogger and other services.

Why not Microsoft?

The finding that Microsoft is a better privacy performer than Google is also likely to be contentious. Microsoft was awarded "orange" status, two bands better than Google's position. However it is important, for the sake of clarity, to note that Windows Live Space received the more negative "red" rating, while Google's Orkut avoided a black rating and was awarded red status.

The true difference between Google Inc and Microsoft Corp can be defined not so much by the data practices and privacy policies that exist between the two organizations, but by the corporate ethos and leadership exhibited by each. Five years ago Microsoft could reasonably be described as a fundamental danger to privacy. In more recent times the organization appears to have adopted a less antagonistic attitude to privacy, and has at least structurally adjusted to the challenge of creating a privacy-friendly environment.

It is true that even during this more recent period there have been notable privacy disasters, particularly with WGA. It is equally true that Microsoft has failed to achieve the level of transparency that it proclaims to embrace (for example in withholding the length of time that data is retained). These instances have been compounded by a failure of oversight and management. However Microsoft has at least put in place the beginnings of a framework for responsible privacy practice and has created a corporate vision, cloudy though it may be. The organization appears now to be particularly sensitive in the most part to privacy issues and some parts of Microsoft have even pursued the concept of privacy as a market differentiator. We have no evidence that Google has achieved this level of awareness or development.

However we are aware that – in the words of the executives – "ad space is now the only game in town," and with Microsoft needing to play catch-up with Google there is a real threat that the organization could abandon privacy reforms in favor of ad revenue – or at least divert funds away from real protection and toward PR. The 2008 rankings will identify whether this fear will be realized.

Key findings

While there may be a temptation to focus criticism on Google's privacy performance, it is important to note that not one of the ranked organizations achieved a "green" status. Overall, the privacy standard of the key Internet players is appalling, with some companies demonstrating either wilful or a mindless disregard for the privacy rights of their customers. Even the better performing companies create lapses of privacy that are avoidable. With minimal effort most organizations can improve their privacy performance by at least one grade.

The current frenzy to "capture" ad space revenue through the exploitation of new technologies and tools will result in one of the greatest privacy challenges in recent decades. The Internet appears to be shifting as a whole toward this aim, and the opportunity to create market differentiators based on responsible privacy may diminish unless those avenues are explored immediately. We have been impressed by the good work being achieved by some sites, but consumers are right to feel aggrieved when companies fail to adopt the best privacy tools that are available.

On the basis of the evidence we have seen from this study, there is no excuse for any organization to ignore the opportunity to create strong privacy protections. The technologies are available, the expertise is abundant, and the market appears willing to favour sites that treat their customers with respect. We hope that the 2008 rankings will reflect this potential.