

**European Parliament Committee on Civil Liberties, Justice and Home Affairs
Public seminar: Data Protection on the Internet, 21 January 2008**

Intervention by Peter Fleischer, Global Privacy Counsel, Google

Dear Chairman,
Dear Members of the European Parliament,
Ladies and Gentlemen,

Thank you for the invitation to participate today. My name is Peter Fleischer. I work as Google's Global Privacy Counsel, based out of Google's Paris office. My job is to help drive Google's commitment to privacy protections by advocating for strong and innovative user privacy safeguards, both inside our company and across our industry. Today I'm going to discuss Google's approach to privacy generally, as well as the types of data we collect for purposes of providing services and serving relevant advertising to our users. We are confronting some of the hardest issues of privacy on the Internet. And in many ways, we're leading our industry. We're committed to working with leading stakeholders around the world to develop strong privacy protections for Internet users everywhere.

At Google, our success depends on trust. If our users don't trust us, they won't use our services. And they won't trust us, if we don't protect their privacy. Because we support open platforms, our users are just one click away from switching to a competitor's services. This means that we have to work every day with every product to earn their trust and their business. At some companies, engineers build a product and then lawyers figure out afterwards how to make it privacy-friendly. At Google, we design privacy protections into our products from the very beginning. At Google, we believe that privacy is a requirement for the entire industry. At Google, we are committed to engaging in privacy dialogue with stakeholders around the world.

At the bedrock of our privacy approach are two fundamental principles:

- **Transparency:** We are upfront with our users about what information we collect and how we use it so they can make informed choices about using our services. We have been an industry leader in finding innovative ways to educate users about privacy. For example, we recently launched a Google Privacy Channel on YouTube where we feature videos that explain our privacy policies in simple, plain language. In line with the long-standing European requirements to provide clear and effective privacy notices to consumers, our privacy channel includes video tutorials about server logs and cookies, as well as privacy tips from Google engineers and product managers on how to use privacy settings in our products like Blogger, Picasa, and Calendar to limit the number of people who can view the information shared through these services.
- **Choice:** We design our products in a way that gives users meaningful choices about how they use our services and what information they wish to choose to provide to us. For example, our Web History service lets users view, pause, or delete their entire search history with just one click, and our Google Talk instant messaging service includes an "off the record" feature that prevents either party from storing the chat. In addition, we give users the option of using many services, including our flagship search engine, without registering or logging in. And we've designed many of our services, like Gmail, to capture minimal user information. Unlike many of its competitors, Gmail doesn't require users to provide detailed demographic profiles to open an account.

Our privacy innovation doesn't stop at transparency and choice; innovation also typifies our approach to other privacy protections. For example, last year we became the first leading search engine to announce a finite logs retention policy of 18 months, after which we anonymize the

Internet Protocol addresses and cookies stored in our log files. (Cookies are small text files stored by a web browser to retain a user's site preferences, such as the preferred language). Our retention policy is designed to continue improving our services and protecting our systems' integrity and security, and further protecting user privacy through finite retention. Permit me a moment to address each of these factors.

First, we work constantly to improve the quality of our search services. Analyzing logs data is an important tool to help our engineers refine search quality and build helpful new services. Take the example of Google SpellCheck. If you were to search for 'David Beckam' without the "h", and gotten correct results for 'David Beckham,' that is a quality improvement that is the result of logs analysis. Similarly, we analyze these search patterns over time to detect and prevent things like phishing, spam or click fraud. And, lastly, these logs represent our business records; it is important that we have complete records for a variety of business reasons.

We are committed to privacy and are constantly improving our privacy policies. That's why we recently made the decision not to retain IP addresses and cookie IDs indefinitely. We reduced our cookie lifespan from 30 years to 24 months, a significantly shorter lifespan than the cookies of many other companies. It is also one that leads to privacy innovation not only at Google but throughout our industry. We are pleased that other search engines – including Microsoft and Yahoo – followed our lead by setting their own data retention policies.

Let me turn now to Google's advertising offerings. Advertising is a critical component of the web ecosystem. The rapid growth of the Internet -- and the promise of future growth -- has been driven primarily by advertising. Online advertisers and web publishers, including small businesses, websites and bloggers, are flourishing because of the ability to reach their individuals throughout Europe and the World in an effective and efficient way. And billions of euros of information, services and software applications are provided today for free, or nearly free, because of online advertising.

At Google, we've created a very robust ad platform that uses a very narrow range of user data to target ads. We derive most of our advertising revenues from our AdWords and AdSense programs, which target ads contextually based on the words that a user is searching for or viewing at a given moment.

More specifically, we serve AdWords ads based on recent search queries entered by the user, the language we believe the user performing the search prefers (based on the Google domain used, user settings, and/or the language of the search query entered by the user), and the IP address of the computer used by the user to ascertain an approximate geographic location. If a user is viewing content on a Google Network member's web site, we serve AdSense ads based on the content of the page (e.g., an article about golf), the language of the page's content, and the IP address of the computer used to ascertain an approximate geographic location. Thus, although we may consider a user's recent prior search queries in order to determine what information is relevant to the user at that moment, our current advertising offerings do not serve ads based on long-term profiles of web pages viewed.

With approval of our DoubleClick acquisition pending, we're taking a closer look at third-party ad serving (a new business for us), and evaluating current industry practices, as well as potential innovations to strengthen privacy protections in this space. In line with best practices adopted by the ad serving industry, our new test ad server includes a cookie opt-out mechanism, empowering users to choose whether to have an advertising cookie placed on their computers. If users do accept ad serving cookies, those cookies will expire after two years. In addition, our industry-leading decision to anonymize logs data after 18 months will encompass any ad-serving logs. When it comes to experimenting with new online ad technologies and approaches, we're exploring providing better forms of notice within ads to help users understand who is behind the ads they

see. Like all experiments, these ideas may or may not work out, but at Google, we're committed to doing our part to create privacy safeguards for online ad serving.

Some have raised the concern that Google and DoubleClick would merge their databases. Let me be clear: DoubleClick does not own its customers' data. As far as DoubleClick is concerned, it can only use the data it processes from serving ads to provide aggregate reporting, like click-through rates for different ad formats. The data is owned by the publishers or advertisers that DoubleClick works for. DoubleClick customers would be very displeased if one tried to undo their contractual relationships by sharing information between advertisers.

We believe that the real question is not about the quantity of data, but about the quality of data practices. It is a question of responsible notice, collection and use of data by all market actors, whether large or small. We believe that the entire industry needs to work together to develop solutions to the consumer privacy issues presented by online advertising. That's why we're actively participating in efforts to help industry establish and improve self-regulating mechanisms, and we support efforts to develop industry-wide privacy standards in this space. For example, we recently participated in the US Federal Trade Commission's Town Hall on behavioral targeting and are currently studying the principles proposed by the FTC to guide data collection practices in this space.

The FTC proposals can serve as a good foundation for establishing self-regulatory practices as they touch on each important privacy and security issue implicated in online advertising: transparency, consumer choice, security, and protection of sensitive personal data such as health condition or sexual orientation. We will engage with the FTC and industry to work through these principles. In that process we expect to raise concerns and offer solutions to certain issues. For example, we believe that the principles would be stronger if they focused on personally identifiable information.

I leave you with three final thoughts.

First, for Google privacy did not begin and does not end with our acquisition of DoubleClick. And we believe that privacy for legislators, regulators, privacy groups, and other stakeholders shouldn't begin or end with Google. Privacy is a serious issue that spans several industries from financial services to entertainment to e-commerce, and that ought to be addressed holistically in the interest of individuals throughout Europe and the World. One particular company -- and certainly one particular merger -- should not be singled out.

Second, online technologies are rapidly evolving, and issues of online data collection, use and retention are relevant to an ever-expanding number of companies operating on the Internet across multiple industries. It is critical for us, and for the entire industry, to ensure that privacy safeguards keep pace with technological change in order to maintain the trust that is essential for future growth. We look forward to continued engagement with this Committee and with privacy stakeholders around the world, including the Article 29 Working Party as well as many of the European Data Protection Authorities, as we pursue our common goal of improving privacy protections for all Internet users.

Third and finally, Google has worked hard to support the creation of global privacy standards that would accomplish important goals, such as building consumer trust and protections, giving clear rules to business, creating a uniform framework for privacy (which would create consistent levels of privacy from one jurisdiction to another), and putting penalties in place to punish and dissuade bad actors. Privacy practices on the Internet cannot stop or change at borders. That's not how the Internet was designed. In the area of online advertising, the industry cannot develop one set of self-regulatory principles in Washington and another in Brussels. As the proposed FTC principles are broadly in line with longstanding EU data protection principles, we perceive them as

a contribution to developing global principles. Let's work together, industry, regulators, government leaders and privacy advocates, to develop a set of privacy principles that will work across the globe, ensuring solid privacy protections for Internet users everywhere. Your hearing today in the European Parliament certainly is an important step toward the global debate that we need.

Thank you.