

**Beyond Google and evil: How policy makers,
journalists and consumers should talk
differently about Google and privacy**

by Chris Jay Hoofnagle

Abstract

Google has come to symbolize the tensions between the benefits of innovative, information-dependent new services and the desire of individuals to control the contexts in which personal information is used. This essay reviews hundreds of newspaper articles where Google speaks about privacy in an effort to characterize the company's handling of these tensions, to provide context explaining the meaning of the company's privacy rhetoric, and to advance the privacy dialogue among policy makers, journalists, and consumers.

The dialogue surrounding these tensions is unfocused because many policy makers, journalists, and consumers concentrate the debate on whether the company violates its "you can make money without doing evil" corporate motto. This first observation flows to a second: Google's conception of "evil" is tied to the revolution the company brought about in advertising practices, practices that many think are mainstream now. Google is thus missing opportunities to remind the public that its advertising policies have several strong pro-consumer aspects, many of which are lost when "evil talk" is employed. Third, vague privacy rhetoric signals a weak commitment to technical or legal safeguards. Journalists are well suited to remedy this by exercising greater inquiry and skepticism in contexts where Google's privacy representations are non-substantive. Finally, Google heavily relies upon appeals to competition, arguing that those who adopt the company's services engage in meaningful tradeoffs. Quietly shifting practices, lock in, and lengthy data retention periods, however, mean that these tradeoffs must be continually reevaluated. Google should give voice to its competition and tradeoff rhetoric by creating data portability and deletion rights for consumers.

Contents

[Introduction](#)
[How Google "talks" about privacy](#)
[Rethinking Google's privacy rhetoric](#)
[Conclusion](#)

Introduction

How Google “talks” about privacy

“Privacy is important”

When asked to comment on privacy issues, Google employees most frequently respond with some variation on “privacy is important.” [4]. Google does this 15 times in the sample of news articles, and in three of the company’s versions of its privacy policy. “Privacy is important” is invoked when discussing many different privacy issues presented, including the DoubleClick merger, 23andme, Google Street View, behavioral advertising issues, and the problem of personal information appearing online. In many articles, Google makes similar representations: “trust is important,” [5] eight times; “security is important,” two times.

Google’s “privacy is important” talk is common among chief privacy officers [6]. Avoiding the “creepiness factor” is a principal reason for employing such rhetoric. The more privacy is at issue, the more likely that a consumer will feel that a product is creepy and avoid it. Thus, stating that “privacy is important” reassures consumers without opening a substantive dialogue about data practices [7].

“Privacy is important” talk effectively operates on several consumer biases, and Google is smart to employ it. As Machiavelli noted in the sixteenth century, “... men in general judge rather by the eye than by the hand, for every one can see but few can touch. Every one sees what you seem, but few know what you are” [8] Machiavelli’s advice to political leaders applies fully in this context because consumers cannot know about any given company’s privacy practices.

The reason becomes clear upon visiting the literature on consumer decision-making in privacy. James Nehf, in his 2007 review of behavioral economics underlying privacy decision making, explains that for consumers to take accurate privacy-preserving decisions, privacy must be salient, but in practice, consumers face hurdles in evaluating privacy [9]. These hurdles make evaluating the information practices of a company practically impossible [10].

Consumers, therefore, must find some proxy for actual privacy practices. Companies like Google are smart to emphasize the quality of their product and services, the good value they represent, and so on, because consumers equate these positive attributes with good privacy practices. This explains why when polled, Americans often choose large, impersonal, highly data-intensive companies with strong reputations for good customer service as being the most “trusted” from a privacy perspective. In 2007, for the second year in a row, Larry Ponemon found that American Express was named as the most trusted company for privacy [11]. Google was included in the top ten.

The reasons why good services translate to high levels of trust are not clearly understood, and even “trusted” companies may engage in problematic privacy activities [12]. Sometimes trust is fleeting, and it always requires continued reevaluation [13]. Consumers do not always have the time [14], or once they have revealed personal information, the ability to effectively revoke a grant of trust.

As with the representation “you can make money without doing evil,” invoking privacy as an important value suffers from two important forms of vagueness, both of which operate on consumers’ optimism biases. The first deals with the meaning of “privacy.” Companies sometimes conceive of “privacy” very differently than consumers. Among many companies, the core meaning of privacy is information security. This limited conception of privacy is concerned with whether personal data can be accessed by unauthorized individuals [15]. Consumers have a much broader conception, and assume that privacy representations carry very strong legal obligations. For instance, Joseph Turow has found that that most consumers think that privacy policies prohibit Web sites from selling personal information [16]. Consumers see privacy representations as a seal or a guarantee of best practices, or as carrying specific legal duties and strong prohibitions, rather than a simple statement of policy [17]. As a result, when consumers hear “privacy is important,” they are likely to optimistically map their own, broad meaning of the word onto Google’s statement. This leaves the gulf between consumers’ and Google’s conception of privacy unexamined.

Second, invoking “privacy is important” avoids making any representation about actual practices, just like “you can make money without doing evil” does not mean that one refrains from incursions into privacy interests or from doing evil. Privacy is important to Google, but it obviously must be subordinated to other values at times. More helpful than “privacy is important” would be some statement of how decisions are made to accommodate competing values, such as advertising revenue, optimization of services, and latency [18].

search companies, and consumers have acclimated to this new height.

Thus, the company's statements about evil have been decontextualized for many users. Recent (post-2000) adopters of the Internet may interpret Google's representations about evil as a general statement of morality, instead of in its original context as an improvement on advertising practices.

At the same time, "evil talk" obscures the substantial consumer benefits from Google's advertising model. Google's policies could limit the potential harms of targeted advertising; give consumers new tools to avoid fraud; dampen the "hucksterism" present in much advertising, making it more relevant and rational; and, curb the age-old problem of the "bait and switch."

Google goes a long way in addressing abuses in targeted advertising, because the company has refused to publish advertisements for a variety of problem products, such as "miracle cures" [24], which newspapers and other media market without apparent reservation. Consumer advocates are very concerned that businesses can use personal information to target advertisements in ways that are manipulative or abusive [25], especially with regard to scammy products. Advocates foresee a day when targeted advertising undermines individuals' autonomy, through leveraging personal information to identify and exploit individuals' weaknesses. However, Google goes some distance in addressing these harms by not allowing ads for some problem products.

Other benefits flow from Google's model. For instance, Google's philosophy of advertising placement may bring more rationality to representations made in marketing. As Saul Hansell reported in the *New York Times* in 2005:

... Google is also preparing to disrupt the advertising business itself, by replacing creative salesmanship with cold number-crunching. Its premise so far is that advertising is most effective when seen only by people who are interested in what's for sale, based on what they are searching for or reading about on the Web. Because Google's ad-buying clients pay for ads only when users click on them, they can precisely measure their effectiveness — and are willing to pay more for ads that really sell their products. [26]

Google's advertising-placing algorithms place a priority on relevance and effectiveness of marketing, which may in the long term limit the creative appeals of advertising copywriters. Consumer advocates and social critics of advertising could see this as a force limiting the manipulative effects of advertising.

Finally, Google and other online advertisers change the economics of an enduring consumer fraud problem — the bait and switch. In the traditional bait and switch, a business attracts customers to a store by advertising a product that it does not intend to actually sell. The business then pitches a different product to customers. Since these customers have sunk costs in traveling to the business, they may be persuaded into buying a different product.

Online advertising changes impose more costs on the fraudulent advertiser, because it is charged when the consumer clicks on the advertisement. The consumer, who has not sunk costs into traveling to a store, can simply press the back button to return to Google and choose a different advertiser.

In this process, Google can track whether these clicks result in a consumer returning to the search engine or a sale, known in the industry as a "conversion." A conversion is obviously a higher-value click, to all parties involved. By measuring and promoting advertisements that lead to conversion, bait-and-switch advertisers will both have to pay for clicks and have their links moved "down the page," where they are less likely to be noticed [27].

These beneficial aspects do not make Google's advertising perfect, nor do they solve all problems that consumer advocates wish to address. But these beneficial aspects are almost never discussed, because the dialogue is focused on "evil" rather than the company's substantive practices.

Tradeoff talk

Google representatives responded to privacy issues by invoking innovation in nine articles. In the context of reporters' privacy questions, appeals to innovation are "tradeoff" arguments. Here, Google is addressing some new privacy problem by appealing to the benefits that the

company's innovation has brought. For instance, the first engagement by the *New York Times* concerned Google's purchase of the Usenet newsgroups. Google addressed privacy concerns by allowing individuals to remove their old posts, and by honoring a self-help remedy created by the prior owner of Usenet. But this first engagement also contained a representation from Google that is characteristic of the company's posture:

"To be able to find things with high accuracy and high reliability really quickly has an incredible impact on the world," Mr. Page said. "Over all, I think that's going to be a net positive, but it is something we worry about."
[28].

Innovation is raised as a privacy tradeoff in the context of data retention, online advertising, Google phonebook, and Google's Web Accelerators service.

Speaking frankly about tradeoffs is important, because fundamentally, Google's business model conflicts with individuals' ability to avoid access to and aggregation of personal information. As Christopher Soghoian argues, the major search engines are dependent upon online advertising for revenue, thus, they have incentives to design services to enable access to and aggregation of personal data [29]. Soghoian explains that some of the most sensitive facts about an individual happen to be the most valuable to the company's advertising model [30]. Furthermore, privacy preserving self-help techniques advocated by consumer groups, such as the Electronic Frontier Foundation, would directly interfere with Google's data collection [31].

Following Soghoian's reasoning, Google has several strong incentives to protect and expand its advertising-supported business model. It must increase opportunities for data collection (think of the expanding array of Google services), it must convince its users that they should search for terms that may be associated with sensitive issues, such as diagnoses of diseases; and, it must discourage or convince individuals that technological self-help is unnecessary. Appeals to how Google's services are innovative and better than competitors' is a prime method for serving these incentives while explaining that the tradeoff answers privacy concerns.

Behavioral advertising is an area where tradeoffs between information collection and better advertising results have been a moving target for Google. The company's rhetoric has shifted, from a position where Google was criticizing behavioral advertising to one where the company quietly adopted behavioral tracking techniques.

The Federal Trade Commission (FTC) has defined behavioral advertising as "the practice of tracking consumers' activities online to target advertising." [32] Under that definition, behavioral advertising encompasses a very broad array of targeting practices, but it is commonly understood that behavioral advertising focuses on tracking user sessions over time, perhaps for hours, months, or even years.

Google initially advocated its search product as a minimally invasive service, because it targeted based upon the user's search string. Accordingly, the targeting of advertisements was ephemeral, related only to the current search. Historically, Google's rhetoric has downplayed user tracking, but it often has warned that its privacy policy allows the company to change its practices. For instance, when Google placed a counter on its home page so that heavy users could track how many times they searched, the *New York Times* reported that Google was not keeping count or tracking the searches of specific users [33]. When Google started its Web Accelerators service and allowed greater personalization of the Google home page, the *Wall Street Journal* reported that Google had no immediate plans to use the data or track individuals, but that it could, consistent with the company's privacy policy, use the data to improve its advertising services [34]. Covering the same issues, the *New York Times* reported: "Google says it has no immediate plans to display advertisements based on, say, the user's location or clicking habits while using the service..." [35] Thus, an individual user evaluating the trustworthiness of Google and considering the tradeoffs of its services would have been exposed to numerous representations that the company was minimizing the data it used to pitch advertising.

As competitors started using more personal information for targeting advertising, Google distanced itself from or criticized competitors for their practices. When Microsoft announced a search advertising model that targeted based upon users' sex, location, and age, the *New York Times* reported: "While Google does not currently use personal data to direct placement of its ads, there is nothing in its privacy policy that precludes it from doing so, said Michael Mayzel, a Google spokesman" [36]. Commenting on behavioral targeting in August 2006, Saul Hansell of the *New York Times* reported:

"Mr. Armstrong [of Google] also challenged the idea that

it was effective to show people advertisements based on what they searched for hours or days earlier: 'Does a user want to see an ad on cars when they are planning their weekend vacation, or do they want to see an ad related to what they are looking at?'"[37]

Again, a user assessing Google's trustworthiness and tradeoffs could conclude that the company's services were less reliant on personal data than others.

Google's posture on behavioral tracking shifted significantly in 2007. In April 2007, the *Wall Street Journal* reported that Google would reorder searches based upon individuals' location and past ad clicking. Google's comment was: "Companies stress that they take users' privacy seriously. 'We know we need to maintain user privacy and make the privacy tradeoffs very clear to the user,' says Google's Ms. Mayer." [38] In March 2008, the *New York Times* reported that, "Google ... says it is unique in that it mostly uses only current information rather than past actions to select ads." [39]

Another step towards behavioral advertising was detected in 2008 by an analyst who closely follows the company. The *New York Times* reported in June 2008 that Gene Munster of Piper Jaffray tested the company's search engine by submitting a series of queries [40]. Google confirmed a change in approach:

Nick Fox, a director of product management who looks after ads on Google's search site, said the company was now testing the use of more search queries in its ad targeting. He did not describe how it was doing that. But Internet experts said that it was most likely using its cookies.

Mr. Fox said that Google's approach was different from what Yahoo, AOL and others call behavioral targeting. Those companies look at what a user did a few days earlier to show them ads about the same topic today. Google says it believes that search engine advertising is most effective if it relates to what the user has most recently searched for [41].

The line between searches generated on single, ephemeral actions by the user and those tailored based on historical user action seems to have been crossed. Google said in this article that it is different than its competitors, but the difference is no longer one of kind but rather of degree. Google now personalizes searches, "mostly uses only current information" to target advertisements [42], analyzes referrers logs to target advertisements [43], and now, looks at a few past searches.

The weaknesses of tradeoff talk are made clear by Google's sliding down the slippery slope towards behavioral advertising. The user who evaluated the tradeoffs from 2000–2006 could rely upon unqualified statements about Google's aversion to behavioral targeting. Google's quiet shift from this position to its current practices probably was opaque to most users. Users who did notice are in a different position in evaluating tradeoffs. They have already used Google for years and may have some lock in from adopting the company's many services. Tradeoff talk thus places the user in the position where practices must continually be reevaluated; when these practices change, one must ask whether revocations of trust can be effective, because individuals have no right to require a service to erase personal data collected about them.

Tech talk

Representations about "technological safeguards" were invoked nine times by Google; a related argument, "computers, not people, processing data" was used three times. Both arguments were raised when questions about Google's Gmail service arose in 2004. That service targets advertisements based upon the content of e-mail. Google's Wayne Rosing was quoted as saying, "We have a lot of code that tries to prevent inappropriate ads from being displayed", and in response to concerns that Google would read individuals' e-mail messages, Rosing said, "It's computers doing processing." [44] Technological safeguards were invoked with respect to concerns about Google's GDrive, Google Desktop, and the privacy of search queries.

Technological safeguards offer significant promise for allowing use of personal information

while reducing risks of noxious uses of data. But this survey of salient news articles does not reveal innovative or even interesting privacy-enhancing technologies [45]. Google has missed obvious opportunities to include privacy enhancing technologies in their products (providing encryption in Gmail, for instance), and when it has made technological interventions, they are symbolically strong but practically limited. A recent example is Google's recent announcement that the company is anonymizing search logs after just nine months [46]. Christopher Soghoian characterizes this intervention as "snake oil" and "laughable:" the company is only erasing a very small portion of users' IP addresses, and it is still retaining uniquely identifiable cookie values [47].

Sometimes, Google's technological safeguards completely miss the "privacy point." Consider Google Talk, Google's instant messaging service. By default, Google Talk stores the content of all chats in the user's Gmail account. Thus, many instant message conversations, often informal and expected to be ephemeral, become memorialized forever.

To address this, Google allows users to go "off the record," a function that disables storage of instant message chats [48]. This function may be useful for some users, but it misses the larger privacy point — whether Google saves a copy of the chat on its servers. If Google maintains a copy, it can be obtained without the knowledge of the users by civil litigants and law enforcement under diminished U.S. Fourth Amendment standards. Whether Google maintains copies is not addressed in a privacy video created by Google [49] to promote the feature nor in the Google Talk privacy policy [50]. Google's Web History function suffers from a similar limitation — one can remove logs of searches and other uses of Google from their account, but a copy resides on Google's servers [51].

Furthermore, the name Google chose for Google Talk's technological intervention is very similar to an effective privacy-enhancing technology known as "Off-the-Record Messaging" (OTR) [52]. Google Talk's "off the record" function is a pale imitation of OTR. Those who use Google's version are simply hiding the ball (from themselves). The result is that the user may perceive that the underlying privacy problem is solved, but in reality, it was simply obscured. In comparison, OTR enables cross-platform encryption, authentication of the chat partner, and protection when one loses encryption keys. The result is that if one uses OTR (assuming the encryption is effective), civil litigants and law enforcement have to go to the user, where stronger Fourth Amendment protections are in play, rather than the service provider, to gain access to message content.

Google's privacy rhetoric frames computers as technical safeguards. In three articles, the company responded to privacy questions by arguing that computers, not people, were processing information. In all three situations, Google was discussing Gmail, an e-mail service that analyzes the content of users' messages to tailor advertising.

Is computer analysis of e-mail content less invasive than human review? Google's argument, to say the least, is problematic. First, it assumes that computers are independent of humans. Lawrence Lessig has argued that "Code is law." [53] Google has a tweak on this phrase: "nothing speaks louder than code." [54] Of course, all that code is written by humans. As James Grimmelmann argues in the context of automation of search results, "Who, after all, gave the computer its instructions? The programmer did A computer is just a glorified abacus; it does what you tell it to." [55]

Second, applied in similar contexts, Google's argument could justify mass surveillance. Grand unified database surveillance systems, like Terrorism Information Awareness (TIA), purported to rely upon computer review of events to identify and predict terrorist attacks [56]. TIA, as described by officials, would include a series of technical safeguards to allow computer analysis of very large databases without unauthorized disclosure to humans [57]. Only after suspicious behavior was detected, or where some court intervention was sought, would information be revealed to authorities. Were civil libertarians wrong to criticize this program — because computers, not people — were processing the information?

If the TIA comparison is too attenuated, consider the Internet service provider (ISP) based advertising models proffered by Nebuad or Phorm [58]. Because ISPs touch all of a given user's Internet traffic, they can also scan user traffic for content and serve more relevant advertising. This is all performed by computer, and there are attempts to make the traffic data anonymous to the advertising targeting firm. Despite these technological safeguards, automated, computer-mediated targeting of advertising based on a total account of Internet use remains a highly controversial practice.

If the objection to Nebuad or Phorm shifts to a matter of degree — that ISPs are different because they have access to all of a user's data — what is one to make of Google's ever expanding array of products? A user who employs just a portion of Google's suite of services

reveals a substantial, ISP-like level of data to the company.

Talk on the DOJ subpoena

In August 2005, the U.S. Department of Justice (DOJ) sought a disclosure of all URLs available on Google as of July 2005, and two months of queries submitted by users [59]. This was first reported in the *New York Times* and *Wall Street Journal* in January 2006, along with the revelation that Google's competitors in search had complied with similar requests [60]. But Google very effectively negotiated to narrow the scope of the original request, and made the U.S. government take the company to court to enforce a relatively small release of data [61]. This battle attracted significant attention in the *New York Times* and *Wall Street Journal*: 19 articles were written about the legal conflict and its implications, including three institutional opinion-editorials by the *Journal* and one in the *Times* [62]. The only other legal issue to attract more attention was Google's purchase of DoubleClick (25 articles). When speaking about the DOJ subpoena, Google's representations were more substantive than on other topics — "trust is important" was invoked once, but in many articles, specific risks to privacy were discussed.

In the press, the DOJ subpoena was framed largely as a threat to privacy rights, although other areas of law dominated the legal challenge to release of the data. For instance, privacy was pushed to the end of a five-page letter objecting to the DOJ subpoena. In that letter, Google's privacy argument was:

"Moreover, Google's acceding to the request would suggest that it is willing to reveal information about those who use its services. This is not a perception that Google can accept. And one can envision scenarios where queries alone could reveal identifying information about a specific Google user, which is another outcome that Google cannot accept." [63].

Toward the end of its brief, Google acknowledges that queries can reveal personally identifiable information [64]. It further argued that search queries could be protected by the Electronic Communications Privacy Act, but stopped short of arguing that disclosure would violate that law [65].

Talk on the DoubleClick purchase

Twenty-five articles in the *Times* and *Journal* discussed Google's purchase of DoubleClick, which was announced in April 2007 [66]. An additional 17 articles discussed cookies or tracking of individuals online; thirteen of these articles were published after the announcement of the DoubleClick purchase.

In most of the articles about DoubleClick, privacy issues are discussed but not by any representative from Google. Only two of the articles attribute statements to Google. Shortly after the announcement, Eric Schmidt told the *Times* that Google planned to strengthen protections for privacy, and that, "Our incentive is to get this right because our whole business is dependent on the trust of users." [67] In June 2007, the *Times* reported that Google, responding to critics of the DoubleClick deal, said, "... the online advertising market is young and dynamic, and it expressed confidence that the deal would be approved. The company said it was sensitive to privacy concerns." [68]

Talk on the Viacom lawsuit against YouTube

Six articles in the *Times* and *Journal* covered recent litigation where Viacom and other large owners of video content obtained an order requiring Google to reveal usage logs of its video viewing Web site, YouTube.com. Google objected on privacy grounds to the release of this data, arguing that the combination of user names and IP addresses could identify individuals who used YouTube. The judge rejected this argument, in part because of statements the company had made on its Public Policy Blog concerning the identifiability of IP addresses [69]. The litigants nevertheless agreed to develop a protocol to anonymize the data without specifying the method to be employed [70].

In the post, a Google engineer explained why in most situations, an IP address cannot identify a user [71]. The analysis focuses on the idea that many users have dynamically assigned IP addresses, and thus, their ISP regularly renews the IP address assigned. The engineer concludes, "The reality is ... that in most cases, an IP address without additional information cannot [identify a user]."

Google did not adequately address several counter arguments. First, the post focused on the

idea of whether IP addresses are “personal data.” The adjectives we use to describe data are very important in characterizing information privacy problems. Google’s privacy policies reflect this issue. In the 2000 version of Google’s privacy policy, the company uses the term, “individually identifiable information.” [72] In the 2004 policy, Google uses a slightly different term, one that could be considered narrower: “personally identifying information.” [73] In the 2005 and current privacy policies, Google uses “personal information.” [74].

In this context, the key question is whether identity can be discovered. Thus, the proper inquiry is whether IP addresses are personally *identifiable*. Framing the debate over whether the data are “personal” narrows the inquiry to information that is only about a specific individual, like a Social Security number.

Second, a number of problems flow from the use of the qualification, “without additional information” when attempting to identify a user. Under Google’s reasoning, even data like a Social Security number is not personal because additional information is always needed to link an identifier to a specific individual. Alone, a Social Security number or name does not identify a person.

Third, the technical difficulty of anonymization has been well described by computer scientists, such as Latanya Sweeney and Arvind Narayanan. Sweeney demonstrated that even putatively anonymous databases, such as U.S. Census records, can be reidentified [75]. Google’s position does not address this body of work.

Finally, while the Google analysis attempts to address the “technical realities” of this issue, it ignores the practical reality that those who try to identify others online always use additional information to do so. The process is as simple as using Google search to find a situation where the anonymous speaker used the same username or IP address in an identifiable context. Those seeking to reidentify putatively anonymous databases do not limit themselves from using extrinsic data to discover identities.



Rethinking Google’s privacy rhetoric

“And the manner in which we live, and that in which we ought to live, are things so wide asunder, that he who quits the one to betake himself to the other is more likely to destroy than to save himself; since any one who would act up to a perfect standard of goodness in everything, must be ruined among so many who are not good. It is essential, therefore, for a Prince who desires to maintain his position, to have learned how to be other than good, and to use or not to use his goodness as necessity requires.” [76]

Evil talk is an albatross

Friedrich Nietzsche argued in *Beyond Good and Evil* that “evil” is a relative notion; what is evil varies across time and place [77]. For many, “evil” invokes thoughts of Pol Pot and Stalin. But when Google says, “you can make money without doing evil,” it refers to the company’s “allergy” [78] towards invasive advertising. Google’s “good” refers to the pro-consumer revolution in advertising that the company brought by divorcing commercial interests from search results. The problem is that Google’s revolution is ancient history in Internet time. Many users never experienced or do not remember what searching used to be like, and now have grown to expect organic search results. Thus, for many Internet users, Google’s evil representations are no longer about advertising, but instead have become general purpose statements about the company’s morality.

When “don’t be evil” appears in the *Times* or the *Journal*, it almost always is attributed to the company by the reporter. Of the 14 times evil is invoked, only twice is it attributed directly to a Google employee. In six of these cases, evil is raised in the context of a profile of Google. But in the other cases, the reporter is writing in the context of specific and troubling developments, such as search censorship in China, the DOJ subpoena, or data retention issues. Thus, in many cases, the press uses “don’t be evil” as a way of framing the company as hypocritical outside the context of advertising.

Moreover, in the modern era, saying is that one is not evil is meaningless. It suggests an

unexamined morality; one that finds virtue in good intentions, rather than in good social practice. Confessions of being evil sometimes appear in literature or movies, the realms of fantasy, but rarely in real life does anyone consider oneself to be evil.

Writing on the *Journal's* All Things Digital blog (<http://allthingsd.com/>), John Paczkowski argues:

Let's be honest here: "Don't Be Evil," Google's Hippocratic oath for corporations, was a masterful public-relations gesture when it was first made, but it never changed the increasing risks associated with the company's business operations. Google is a public company, not a public interest. There's really no reason to trust it to do the right thing with your private data [79].

Paczkowski's point is compelling. "Don't be evil" already has become an albatross for the company, one that will weigh more heavily as it expands and finds itself in more morally complex situations than online advertising practices. Participants in the Google privacy dialogue would be best served by abandoning it.

The "evil" albatross detracts from the benefits of Google's advertising model

The evil talk is not only an albatross for Google, it obscures the substantial consumer benefits from Google's advertising model. Because we have forgotten the original context of Google's evil representations, the company should remind the public of the company's contribution to a revolution in search advertising, and highlight some overlooked benefits of their model.

Google's policies could limit the potential harms of targeted advertising; give consumers new tools to avoid fraud; dampen the "hucksterism" present in much advertising, making it more relevant and rational; and, curb the age-old problem of the "bait and switch."

Google's actions in this space could be labeled paternalistic, but the reality is that tens of millions of Americans are victims of consumer fraud each year. The FTC found in 2005 that 13 percent of Americans were victims of some type of consumer fraud [80]. Google's policies limit the ability of the many common fraudsters from reaching its customers.

Google could go farther. According to the FTC, weight loss products are the most frequently used scheme to defraud consumers. Google could note this and other trends in consumer fraud, and limit advertising of these types of schemes categorically (as it has done with "miracle cures") or in softer ways (through using disclaimers or through promoting anti-fraud Web sites). Google could allow consumers to tag advertisements as fraudulent, just as eBay allows users to report violations of the site's auction policy.

Vague privacy talk signals weak commitment to protection

Google's privacy representations are most frequently comprised of vague commitments to vague notions of privacy and user trust. Google is talking down to the public with its "privacy is important" rhetoric. Such non-committal talk does not inform the public about the company's values and decision-making processes. It leaves many gaps and unanswered questions, in hopes that consumers' optimism bias and naiveté will fill them with their own values. Consumers thus become unwitting participants in Google's privacy worldview.

Journalists have the opportunity to shape this problem by not taking "privacy is important" as an answer. Follow-up questions could focus upon the relative importance of privacy and when privacy is subordinated to other values. Journalists could even employ hypothetical questions to probe likely conflicts among privacy and other values.

Enable meaningful tradeoffs

Once Google's representations become more specific, consumers will be in a better position to take decisions about tradeoffs. But for tradeoffs to be meaningful, individuals must have the ability to take a choice and revoke it later. Since Google has changed its practices over the years, individuals re-evaluating tradeoffs might be in a situation where they have already adopted a suite of the company's products. Recall that Google disparaged behavioral advertising models, but then slowly started adopting behavioral tracking. A user who started using Google to avoid such practices cannot make a clean break from Google. The tradeoff has already been made; trust has been entrusted, and there is no way to revoke it.

Google could remedy this situation and give real teeth to its tradeoff talk by enabling individuals to take all of their data in Google's services and move it to another provider or

system. To the extent that users' data have been collected in an identifiable way — for instance, through Gmail or a personalized search — users should be able to order that their data be deleted [81]. Without a system to revoke trust, users have no meaningful methods to decide that the Google tradeoff is not worth the costs.



Conclusion

This essay attempts to assist policy makers, journalists, and consumers in beginning a dialogue about Google's privacy practices. In this dialogue, much effort has been wasted considering whether Google is evil, good, or somewhere between. This has caused great obfuscation and distraction. We must get beyond notions of good and evil when thinking about Google. A more focused debate would concentrate on the company's actions and inactions, the choices it makes, and the contexts in which privacy is subordinated to other values. 

About the author

Chris Jay Hoofnagle is director of University of California at Berkeley Law's information privacy programs, an attorney, and senior fellow to the Samuelson Law, Technology & Public Policy Clinic. He is an expert in information privacy law. Hoofnagle co-chairs the annual Privacy Law Scholars Conference. He is licensed to practice in California and Washington, D.C. E-mail: choofnagle [at] law [dot] berkeley [dot] edu

Appendices

Table 1: Google's privacy policies.					
	12 October 1999 version	14 August 2000 version	1 July 2004 version	14 October 2005 version	7 August 2008 version
Number of words	637	674	1,058	1,876	1,943
Sentences per paragraph	2.7	2.9	2.3	2.3	2.3
Words per sentence	19.2	19.8	20.2	23.7	23.5
Percentage of passive sentences	12%	15%	18%	17%	16%
Flesch reading ease (Lower = more difficult)	50.9	50.2	42.4	32.6	32
Flesch-Kincaid grade level (Higher = more difficult)	10.9	11.1	12	12	12

Notes	Retrieved from Internet Archive	Leads with "Google respects and protects the privacy ..."	Leads with "Google respects and protects the privacy ..."	Leads with "privacy is important" Notes Safe Harbor membership	Leads with "privacy is important"
-------	---------------------------------	---	---	--	-----------------------------------

	Google Commenter	23andme	Advertising	AOL Search Terms	Behavioral Profiling	Censorship	Consumer Privacy Law	Cookies/Tracking	Data Retention	DOJ Subpoena	DoubleClick	Google Desktop	Google Gdrive	Google Gmail	Google Groups	Google Health	Google Home Page	Google Maps/Street View	Google Phone	Google Phonebook	Google Street View	Google Use Counter	Google Web Accelerators	Google Wifi	Link to Privacy Policy	Online Investigations	PII Online	Profile of Google	Social Networking	Surveillance	Tech Trends	YouTube-Viacom				
Adam Bosworth																																				
Al Gidari										1																										
Alma Whitten																																		1		
Anne Wojcici	1																																			
Ashok Ramani										1																										
Catherine Lacavera																																		2		
Courtney Hohne																												1								
David Drummond						1																														
David Kramer																																		1		
Douglas Merrill																																		1		
Eileen Rodriguez																										1										
Elliot Schrage						1																														
Eric Schmidt	1	1						1			1																									
J. L. Needham																											1								1	
Jane Horvath							1																													
Joe Kraus																																				
Keith Coleman														1																						
Larry Page															1																					
Larry Yu																										1										
Lauren Maddox																																				
Linda Avey	2																																			
Marissa Mayer				1								1																								
Megan Quinn																																				
Michael Mayzel	1																																			
Nick Fox								1																												
Nicole Wong							1		2	3																										
Peter Fleischer								5																												
Ricardo Reyes																																				1
Sergey Brin	1																																			
Stephen Chau																																				
Steve Langdon			1																																	
Susan Wojcicki													1																							
Tim Armstrong	1	1						1																												
Unidentified	1	2							2	4	1	2	1	3			2	1	1	1	1	1					1	2	2	1				1		
Vint Cerf																																				1
Wayne Rosing														2																						
Total	3	5	5	1	2	2	3	9	9	2	3	1	7	1	3	1	2	1	1	1	1	1	1	2	1	2	4	7	3	4	2		6			

Table 2: Google spokespeople and privacy topics addressed [82].

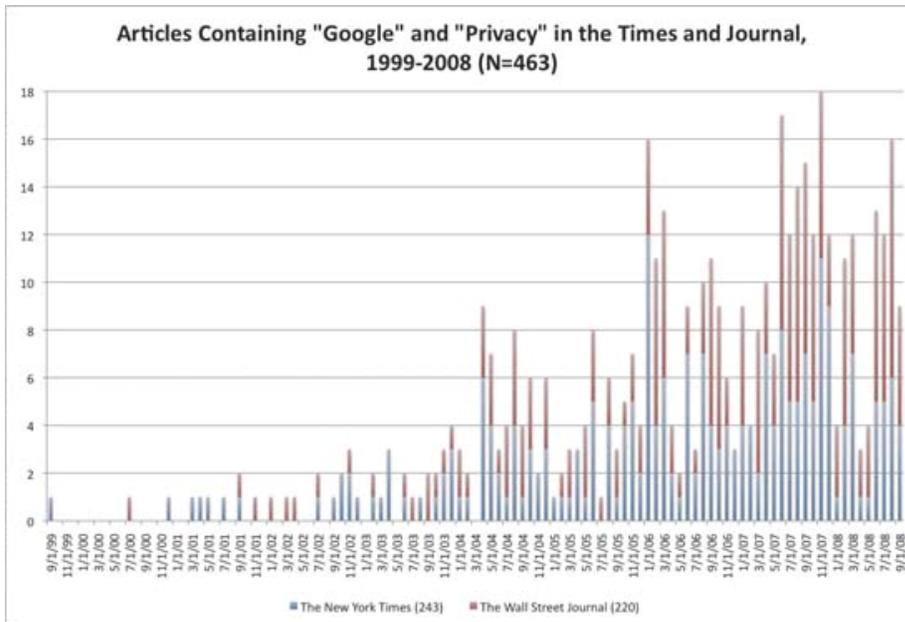


Chart 1: Coverage in the *New York Times* and *Wall Street Journal*.

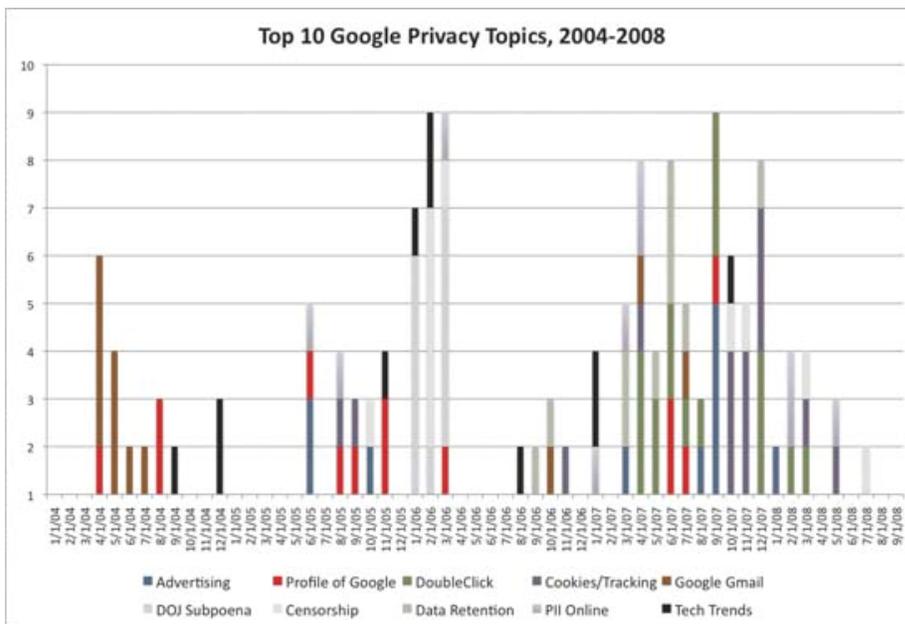


Chart 2: Top 10 Google privacy topics.

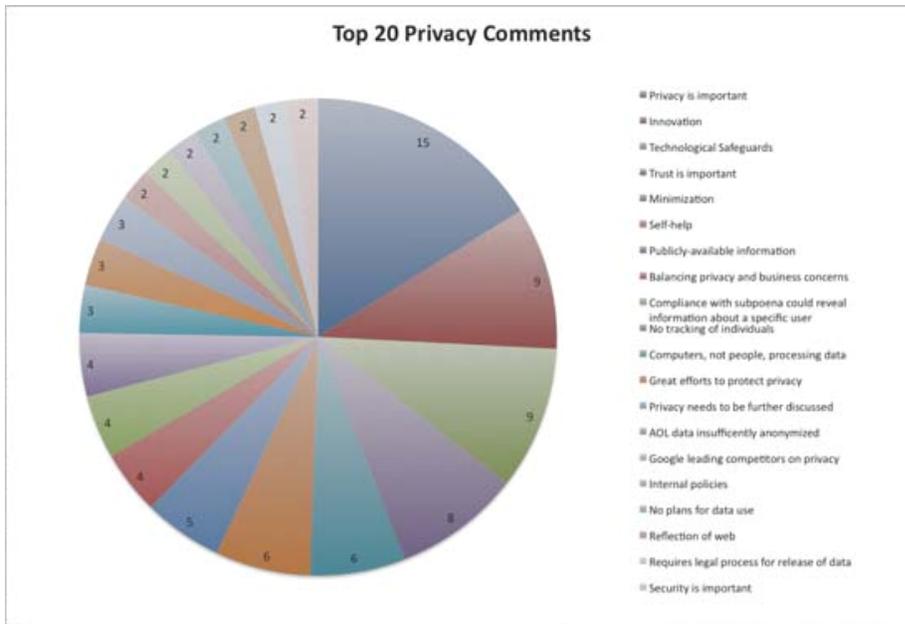


Chart 3: Top 20 Google privacy comments.

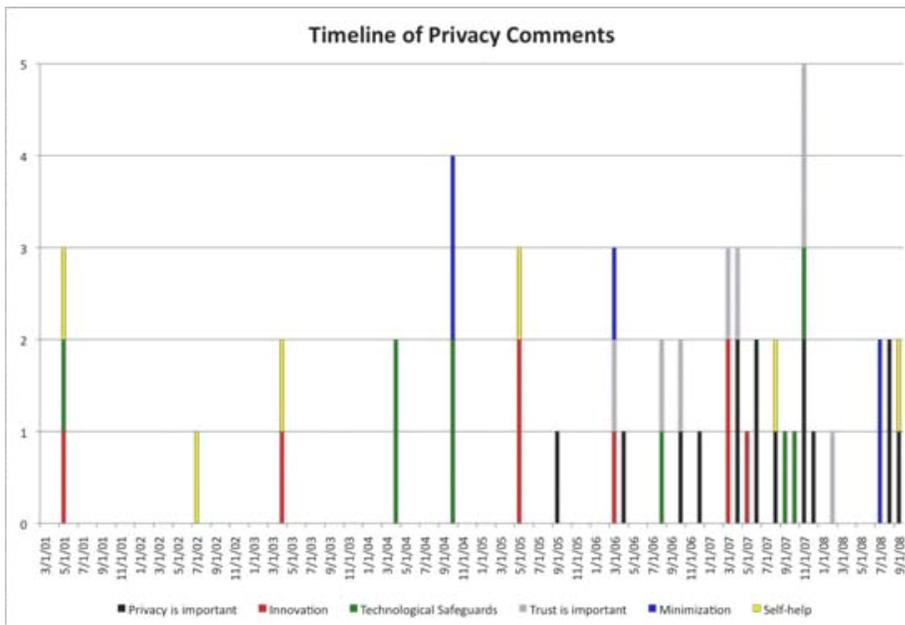


Chart 4: Timeline of privacy comments.

Notes

1. Google, "Company overview," at <http://www.google.com/intl/en/corporate/>.
2. Google, "Our philosophy," at <http://www.google.com/corporate/tenthings.html>.

3. In 126 of the articles, Google was simply referenced as a “resource” where a privacy issue was mentioned. This means that Google is discussed as a service, fact of, or feature of the online world, usually in the context of an article that is not about privacy. For instance, a November 2007 *New York Times* article discusses apartment hunting, and the use of Google to learn more about a property. The article continues to explain that the house hunters value the privacy of their carriage house. Joyce Cohen, “Finding that hidden gem,” *N.Y. Times* (18 November 2007). Frequently, articles classified in this bucket discuss the idea of Googling a term to find a business. The article might then recommend that the consumer check to see if the business has a privacy policy.

4. “Privacy is important” statements are those where Google makes reference to privacy as a value without specifying particular actions taken to protect privacy: *E.g.*, “Privacy and trust are probably the two words that are going to make the Internet the healthiest in the future,” in Louise Story, “F.T.C. takes a look at Web marketing,” *N.Y. Times* (2 November 2007); “A Google spokesman said the company takes privacy seriously but is not currently developing a service to immediately discard search queries,” in Miguel Helft, “Ask.com puts a bet on privacy,” *N.Y. Times* (11 December 2007).

5. *E.g.*, “... our whole business is dependent on the trust of users,” Miguel Helft, “Google profit soars 69 percent for quarter,” *N.Y. Times* (20 April 2007).

6. See *e.g.*, Colin J. Bennett & Charles D. Rabb, *The governance of privacy: Policy instruments in global perspective*, pp. 52–79 (Cambridge, Mass.: MIT Press, 2006).

7. Avoiding creepiness may also explain why Google refused to place a link to its privacy policy from its homepage, until it was required to do so by a California statute. Saul Hansell, “Google, privacy and California,” *N.Y. Times* (2 June 2008). Google originally argued that placing a one-word link to the privacy policy would make its homepage too busy (violating a so-called 28-word rule), but within months added verbiage promoting its new wireless phone (bringing the page to 39 words). Miguel Helft, “Is 39 the new 28 at Google?” *N.Y. Times bits blog* (22 October 2008), at <http://bits.blogs.nytimes.com/2008/10/22/is-39-the-new-28-at-google/>.

8. Machiavelli, *The Prince*, chapter XIII at 130 (Hill Thompson, translator; New York: Heritage Press, 1955).

9. James P. Nehf, “Shopping for privacy on the Internet,” 41 *J. of Consumer Affairs*, 351 (Winter 2007).

10. Consider the limited resource of time as a hurdle. The speed and convenience of ecommerce itself would be squandered if consumers actually read privacy policies, tracked companies’ privacy performance in newspapers, and followed reports by privacy advocates and regulators. Aleecia McDonald and Lorrie Cranor found recently that, “... reading privacy policies carry costs in time of approximately 201 hours a year, worth about \$2,949 annually per American Internet user. Nationally, if Americans were to read online privacy policies word-for-word, we estimate the value of time lost as about \$652 billion annually.” Aleecia M. McDonald & Lorrie Faith Cranor, *The cost of reading privacy policies*, presented at the Telecommunications Policy Research Conference (26 September 2008), at <http://tprcweb.com/files/CostOfReadingPrivacyPolicies.pdf>.

11. Jaikumar Vijayan, “American Express most trusted company for privacy, study finds,” *Computerworld* (28 March 2007), at <http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=privacy&articleId=9014698&taxonomyId=84>.

12. For instance, Hewlett-Packard was ranked in the top five in Ponemon’s 2006 report, dropping to 16 in 2007. Jaikumar Vijayan, “American Express most trusted company for privacy, study finds,” *Computerworld* (28 March 2007), at <http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=privacy&articleId=9014698&taxonomyId=84>. This drop was probably attributable to publicity surrounding Hewlett-Packard’s use of private investigators to intimidate reporters. The point here is that while Hewlett-Packard was so highly rated, in actuality, its agents were engaging in problematic, privacy-invasive investigations of reporters.

13. For example, in order to make consumers feel at ease in conducting more health-related activities online, DrKoop.com leveraged the substantial trust generated from C. Everett Koop’s tenure as Surgeon General. During his time in government, his conviction that tobacco products were harmful drove a number of politically unlikely anti-tobacco interventions. While he was a controversial figure, this tough approach on tobacco was a strong display of integrity against monied political interests. A user of DrKoop.com would assume that medical information entrusted to the site would be shielded from the monied marketing, insurance, and

other interests in the health field. But shortly after DrKoop.com went bankrupt, it attempted to sell its customer database to the worst type of huckster our regulatory system tolerates: a nutritional supplement company. Alorie Gilbert, "Is DrKoop.com taking care of privacy," *ZDNet News* (1 July 2002), at http://news.zdnet.com/2100-9595_22-123846.html.

14. John Palfrey & Urs Gasser, *Born digital: Understanding the first generation of digital natives* at p. 69 (New York: Basic Books, 2008). Observing that, "It's too much to expect any Digital Native to manage a hundred relationships with a hundred companies and other institutions that hold data about her."

15. Colin J. Bennett & Charles D. Rabb, *The governance of privacy: Policy instruments in global perspective* (Cambridge, Mass.: MIT Press, 2006).

16. Joseph Turow, *Americans & online privacy, the system is broken*, Annenberg Public Policy Center (June 2003), at http://www.annenbergpublicpolicycenter.org/Downloads/Information_And_Society/20030701_America_and_Online_Privacy/20030701_online_privacy_report.pdf; Joseph Turow, Lauren Feldman, & Kimberly Meltzer, *Open to exploitation: American shoppers online and offline*, Annenberg Public Policy Center of the University of Pennsylvania (1 June 2005), at <http://www.annenbergpublicpolicycenter.org/NewsDetails.aspx?myId=31>.

17. Chris Jay Hoofnagle & Jennifer King, "What Californians understand about privacy online" (3 September 2008), at <http://ssrn.com/abstract=1262130>.

18. Owen Thomas, "Google CEO has no time for your privacy," *Valleywag* (19 November 2008), at <http://valleywag.com/5093634/google-ceo-has-no-time-for-your-privacy>.

19. John Battelle, *The search*, p. 102, (New York: Penguin, 2005).

20. Saul Hansell, "Your ads here (all of them)," *N.Y. Times* (30 October 2005).

21. John Battelle, *The search*, pp. 91–92, (New York: Penguin, 2005).

22. *Id.* at p. 92.

23. Google, "Our philosophy," at <http://www.google.com/corporate/tenthings.html>.

24. Google, "Advertising policies," at <http://adwords.google.com/support/bin/static.py?page=guidelines.cs&topic=9271&subtopic=9279&hl=en>.

25. See e.g., Charles Duhigg, "Papers show Wachovia knew of thefts," *N.Y. Times* (6 February 2008), at <http://www.nytimes.com/2008/02/06/business/06wachovia.html> ("InfoUSA advertised lists of "Elderly Opportunity Seekers," 3.3 million older people "looking for ways to make money," and "Suffering Seniors," 4.7 million people with cancer or Alzheimer's disease. "Oldies but Goodies" contained 500,000 gamblers over 55 years old, for 8.5 cents apiece. One list said: "These people are gullible. They want to believe that their luck can change.")

26. Saul Hansell, "Your ads here (all of them)," *N.Y. Times* (30 October 2005).

27. Google's system does not address a form of online bait and switch where the business falsely represents that it has inventory of an item in order to entice the consumer into making a purchase.

28. Susan Stellan, "Google's revival of a Usenet archive opens up a wealth of possibilities but also raises some privacy issues," *N.Y. Times* (7 May 2001).

29. Christopher Soghoian, "The problem of anonymous vanity searches" (23 January 2007), at <http://ssrn.com/abstract=953673>. ("If Google can build a higher-quality data set of customer information, they can charge more per advertisement, whilst also gaining a significant market advantage over the other search engines.")

30. *Id.* at 3.

31. *Id.* at 3.

32. "Federal Trade Commission, online behavioral advertising moving the discussion forward to possible self-regulatory principles" at 1 (20 December 2007), at <http://www.ftc.gov/opa/2007/12/principles.shtm>.

33. Lisa Napoli, "Frequent search engine users, Google is watching and counting," *N.Y. Times* (6 October 2003).

34. "Technology brief — Google Inc.: Service to speed Web viewing raises some privacy

concerns," *Wall Street Journal* (5 May 2005).

[35.](#) Bob Tedeschi, "With its home page, Google could get a bit closer to its users," *N.Y. Times* (23 May 2005).

[36.](#) Saul Hansell, "Microsoft plans to sell search ads of its own," *N.Y. Times* (26 September 2005).

[37.](#) Saul Hansell, "Advertisers trace paths users leave on Internet," *N.Y. Times* (15 August 2006).

[38.](#) Jessica E. Vascellaro & Kevin J. Delaney, "Search engines seek to get inside your head — Google, others start to comb users' online habits to tailor results to personal interests," *Wall Street Journal* (25 April 2007).

[39.](#) Louise Story, "To aim ads, Web is keeping closer eye on what you click," *N.Y. Times* (10 March 2008).

[40.](#) Saul Hansell, "Google tries tighter aim for Web ads," *New York Times* (27 June 2008).

[41.](#) *Id.*

[42.](#) Jessica E. Vascellaro & Kevin J. Delaney, "Search engines seek to get inside your head — Google, others start to comb users' online habits to tailor results to personal interests," *Wall Street Journal* (25 April 2007).

[43.](#) Saul Hansell, "Google tries tighter aim for Web ads," *New York Times* (27 June 2008).

[44.](#) Katie Hafner, "In Google we trust? When the subject is e-mail, maybe not," *N.Y. Times* (8 April 2004).

[45.](#) For instance, with respect to Google Desktop, the company was developing password protection in order to deal with the problem of finding other users' information while using Desktop Search. Kevin J. Delaney, "New search software raises privacy issues; Recording IM sessions," *Wall Street Journal* (27 October 2004).

[46.](#) Google, "Another step to protect user privacy" (8 September 2008), at <http://googleblog.blogspot.com/2008/09/another-step-to-protect-user-privacy.html>.

[47.](#) Chris Soghoian, "Debunking Google's log anonymization propaganda," *CNet* (11 September 2008), at http://news.cnet.com/8301-13739_3-10038963-46.html.

[48.](#) Google, "Chat 'off the record' — Google privacy tips" (19 December 2007), at <http://www.youtube.com/watch?v=HBwkvnyLXDE>.

[49.](#) Google, "Chat 'off the record' — Google privacy tips" (19 December 2007), at <http://www.youtube.com/watch?v=HBwkvnyLXDE>.

[50.](#) Google, "Google Talk privacy notice," at <http://www.google.com/talk/privacy.html>.

[51.](#) Google, "Web History privacy notice," <http://www.google.com/history/privacy.html>.

[52.](#) "Off-the-Record Messaging," at <http://www.cypherpunks.ca/otr/>.

[53.](#) Lawrence Lessig, *Code and other laws of cyberspace* (New York: Basic Books, 2000).

[54.](#) Steve Lohr & Miguel Helft, "Clash of the titans," *N.Y. Times* (16 December 2007).

[55.](#) James Grimmelman, "The Google dilemma," *N.Y.L.S.L. Rev.* (forthcoming).

[56.](#) "Department of Defense, Office of the Inspector General, Terrorism Information Awareness Program — Report No. D-2004-033," (12 December 2003), at <http://www.dodig.osd.mil/audit/reports/FY04/04033sum.htm>.

[57.](#) *Id.* at pp. 9-10.

[58.](#) See e.g., Paul Ohm, "The rise and fall of invasive ISP surveillance" (30 August 2008), at <http://ssrn.com/abstract=1261344>.

[59.](#) See "Declaration of Joel McElvain" at 4, *Gonzales v. Google, Inc.*, 234 F.R.D. 674 (N.D. Cal. 2006).

[60.](#) Katie Hafner & Matt Richtel, "Google resists U.S. subpoena Of search data," *N.Y. Times* (20 January 2006).

[61.](#) 234 F.R.D. at 679.

[62.](#) "Google's half victory," *Wall Street Journal* (21 March 2006), at p. A14; "Hot topic: Searching for Google," *Wall Street Journal* (18 March 2006), at p. A8; "... And Google at home," *Wall Street Journal* (30 January 2006), at p. A18; "Fishing in cyberspace," *N.Y. Times* (21 January 2006), at p. 12.

[63.](#) "Declaration of Joel McElvain" at 17, *Gonzales v. Google, Inc.*, 234 F.R.D. 674 (N.D. Cal. 2006).

[64.](#) "Google's opposition to the government's motion to compel" at 18, *Gonzales v. Google, Inc.*, 234 F.R.D. 674 (N.D. Cal. 2006).

[65.](#) "Google's opposition to the government's motion to compel" at 18–21, *Gonzales v. Google, Inc.*, 234 F.R.D. 674 (N.D. Cal. 2006).

[66.](#) Louise Story & Miguel Helft, "Google buys an online ad firm for \$3.1 billion," *N.Y. Times* (14 April 2007).

[67.](#) Miguel Helft, "Google profit soars 69% for quarter," *N.Y. Times* (20 April 2007).

[68.](#) Steve Lohr, "Inquiry into deal," *N.Y. Times* (2 June 2007).

[69.](#) "Opinion and order" at 13 in *Viacom International et al. v. Youtube et al.*, 07–CIV–2103 (LLS), (S.D.N.Y. 1 July 2008).

[70.](#) Jessica E. Vascellaro, "YouTube suit sets protocol to shield IDs," *Wall Street Journal* (21 July 2008).

[71.](#) Alma Whitten, "Are IP addresses personal?" *Google Public Policy Blog* (22 February 2008), available at <http://googlepublicpolicy.blogspot.com/2008/02/are-ip-addresses-personal.html>.

[72.](#) Google, Inc., "Archive: Privacy policy" (14 August 2000), at http://www.google.com/privacy_archive_2000.html.

[73.](#) Google, Inc., "Archive: Privacy policy" (1 July 2004), at http://www.google.com/privacy_archive_2004.html.

[74.](#) Google, Inc., "Archive: Privacy policy" (14 October 2005), at http://www.google.com/privacy_archive.html; "Google, Inc., Privacy policy" (7 August 2008), at <http://www.google.com/privacypolicy.html>.

[75.](#) "... 87% (216 million of 248 million) of the population in the United States had reported characteristics that likely made them unique based only on {5–digit ZIP, gender, date of birth}. About half of the U.S. population (132 million of 248 million or 53%) are likely to be uniquely identified by only {place, gender, date of birth}, where place is basically the city, town, or municipality in which the person resides. And even at the county level, {county, gender, date of birth} are likely to uniquely identify 18% of the U.S. population. In general, few characteristics are needed to uniquely identify a person." Latanya Sweeney, *Uniqueness of Simple Demographics in the U.S. Population*, Laboratory for International Data Privacy (2000), at <http://privacy.cs.cmu.edu/dataprivacy/papers/LIDAP-WP4abstract.html>.

[76.](#) Machiavelli, *The Prince* Ch. XV at pp. 115–6 (Hill Thompson, translator; New York: Heritage Press, 1955).

[77.](#) Friedrich Nietzsche, *Beyond Good and Evil: Prelude to a Philosophy of the Future* pp. 74–92 (Marion Farber, translator and editor; New York: Oxford University Press, 1998).

[78.](#) John Battelle explains that the Google founders' skepticism of advertising, described as an "allergy" by an early investor, caused a delay in finding a sustainable funding model for the company. John Battelle, *The search*, p. 92, (New York: Penguin, 2005).

[79.](#) John Paczkowski, "Digital daily: Selective search privacy," *Wall Street Journal* (18 June 2007).

[80.](#) Federal Trade Commission, "Consumer Fraud in the U.S.: Second FTC survey" (October 2007), available at <http://www.ftc.gov/opa/2007/10/fraud.pdf>.

[81.](#) In April 2007, John Battelle called for data portability and a deletion right, among other consumer protections. John Battelle, *The Data Bill of Rights*, *John Battelle's Searchblog*, at <http://battellemedia.com/archives/003575.php>.

[82.](#) This table only reflects articles where someone from Google was quoted, not all articles

covering a certain topic.

Editorial history

Paper received 14 December 2008; accepted 14 March 2009.



"Beyond Google and evil: How policy makers, journalists and consumers should talk differently about Google and privacy" by Chris Hoofnagle

is licensed under a [Creative Commons Attribution-NonCommercial-No Derivative Works 3.0 United States License](https://creativecommons.org/licenses/by-nc-nd/3.0/us/).

How policy makers, journalists and consumers should talk differently about Google and privacy by Chris Jay Hoofnagle

First Monday, Volume 14, Number 4 - 6 April 2009

<http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/rt/prINTERfriendly/2326/2156>