IENG-400 Technology and Global Issues

By Zainab Ebrahimi

Tracking Intentions: Internet Privacy Issues

We live in an Internet driven society, so much so that we depend on it for almost everything, from checking the weather or watching a movie to reading the news and answering emails. And to a certain extent we trust in it almost blindly. Since it’s development, the Internet was always an open place to share and interact, gain knowledge and create. It was a free and democratic space. And as the popularity of the Internet has grown the cyberspace invaded the private space or maybe the private space invaded the cyberspace. In the end, the web is filled with tons of information on us. Today, data entered into forms or contained in existing databases can be combined almost effortlessly with transaction records as well as records of an individual's every click through cyberspace (L. Cranor). Not to mention the huge boom of social networks like Facebook and twitter, storing all your pictures, likes and conversations. Who has access to all this information? What are they doing with this information? Is our information secure? Who else can access the information and under what conditions? All these questions are asked because obviously privacy on the Internet is dead.

**PRIVACY**

Privacy is often thought of as a moral right or a legal right. But it's in our case more useful to identify privacy as the interest that individuals have in sustaining a personal space, free from interference by other people and organizations (Clarke). Privacy issues are further intensified now that the World-Wide Web makes it easy for new data to be automatically collected and added to databases (L. Cranor). Privacy concerns relate to personally identifiable information, that is, information that can be used to uniquely identify, contact, or locate a specific individual person. (Tene). From a privacy standpoint that person X is a heroin-addicted, schizophrenic Satan worshipper, who earns $10,000 a month, half of which he spends on diet pills is almost irrelevant, as long as an individual person is not linked to the information. Federal privacy legislation protects personally identifiable information in a number of contexts, such as health information, financial data, or credit reports, but what about the rest? Could specific individuals be identified according to the data in their search query logs?

Google, Yahoo, AOL and many other search engines and websites do. We’ll stick to Google, as an example. Google is an informational gatekeeper, harboring previously unimaginable riches of personal data. Billions of search queries stream across Google servers each month, the aggregate thought stream of humankind online. (Tene). Google archives all search queries linked to a specific IP address and the hyperlinks users click on after obtaining their search results. In its privacy policy, the company states:

[O]ur servers automatically record information that your browser sends whenever you visit a web site. These server logs may include information such as your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser.[[1]](#footnote-1)

Google argues that the retention of search query logs is critical to its ability to operate and improve its services. Google’s task of having to guess what a user intends, essentially "read there mind" is pretty challenging. We’ll give Google that much. As Google co-founder Larry Page puts it, "[t]he perfect search engine would understand exactly what you mean and give back exactly what you want."[[2]](#footnote-2) Who can disapprove of optimizing search results? But, really "link by link, click by click, [Google] is building possibly the most lasting, ponderous, and significant cultural artifact in the history of humankind: the Database of Intentions (Battelle) ". Google’s Database of Intentions is an invaluable asset. No wonder in 2008 Google merged with Doubleclick leading provider of Internet-based advertising. So, Google also analyzes search query logs for revenue generating purposes! Google, after all, is an advertising company. Google's chief executive officer, Eric Schmidt, stated: "If we target the right ad to the right person at the right time and they click it, we win." Targeting "the right ad to the right person at the right time" requires knowing the users and knowing the users means analyzing their search history. A leading advocate for human rights, Privacy International, recently ranked Google's privacy practices as the worst out of a group of more than 20 leading Internet service providers, including Microsoft, Yahoo, Amazon, and eBay. (Simpson) Privacy International describes Google as "an endemic threat to privacy."

Search engine’s databases of intentions are a virtual honey pot for various third parties, ranging from national security and law enforcement officers to hackers and identity thieves (Tene). Fortunately for us, search engines don’t sell users' personally identifiable information to third parties, but certain third parties can—and in fact do—try to obtain user personally identifiable information from search engines through the legal process. First and foremost, the government may use search query logs for national security and law enforcement purposes, including the prevention, detection, and prosecution of crimes (Elkin-Koren). Clearly, a user searching for terms such as "illegal child pornography" or "prepare bomb attack" should permit law enforcement interference. And in fact, governments tend to emphasize the most severe criminal activities, such as pedophilia, terrorism, and organized crime, when seeking authority to access user search query logs. (McCullagh) Few would dispute the imperative to provide government with all necessary tools to combat such terrible acts. But, the scenario becomes muddier when the government seeks to access search query logs of individuals who search for "how to cheat IRS." And without notice that may lead to the criminalization of search terms, such as "Falun Gong" or "democracy Tiananmen," like in China. The police is using search engine records as evidence in a variety of cases, from homicide to wireless hacking. A full search warrant would enable law enforcement officers to access search engine data. *The New York Times* reported that Yahoo! alone responds to approximately 1,000 such criminal search warrants each month.

Grabbing a terrorist before he bombs a passenger jet is one thing. It is quite another thing to arrest a teenager who runs Google searches for "kill guns," "prozac side effects," "brutal death metal bands," and "blood gore," and is therefore profiled by a data mining program as a potential "Columbine shooter." You might not want such a teenager to sit next to your daughter or son in class; but incarcerating him based on his Google searches? In essence it’s applying guilt based on thoughts or intentions as opposed to actions (Taipale). Collecting data on terrorist or possible gun shooters is one thing, what about attempts to identify online users who violate copyright law or to use search engine logs to use in legal cases of divorce, defamation, employment disputes, and shareholder actions? Some government and corporate executives show the increasing social problems related to the internet, and the flaws in security, as evidence that privacy is not only dead, but ought to be dead. They perceive the public is not to be trusted. (Clarke)

I used Google as an example, but other corporations and organizations are also keeping track of your information, like Facebook and Twitter, your Internet service providers (FIOS, Cablevision, Time Warner, etc.), even major e-commerce websites.

We can agree that now more than ever we need an informed Internet user community that’s aware of these threats to their rights, liberties and securities. Once informed of the threat, then what? One option is to divulge as little as possible and become as anonymous as we can. Or, as Brin argues that since the use of technology is imperative and almost irresistible, privacy protections are futile. He proposes that to achieve privacy, rely on freedom, not secrecy. Brin asks: “Who will keep a watch on the watchers? The watched.” With global openness, the powerful will be just as subject to visual and data surveillance as everyone else. The police would be judged by the viewers whom- using the Internet - watch them watching others.

Regardless of which option we chose, there is an imperative need to open the debate to the community. Privacy protections demand a sincere approach, involving individuals, organizations, industry associations, and governments, operating to construct a legislative framework.

# Bibliography

Battelle, John. "The Database of Intentions." 13 Nov 2003. John Battelle Search Blog. <http://battellemedia.com/archives/000063.php.>.

Brian, D. The Transparent Society. Addison-Wesley, 1998.

Clarke, Roger. "Internet privacy concerns confirm the case for intervention." Communications ACM 42 (1999): 60-67.

Cranor, L. "Internet privacy: A public concern." netWorker (1998): 13-18.

Cranor, Lorrie Faith. "Internet Privacy." Communications ACM 42.2 (1999): 28-38 .

Elkin-Koren, Michael D. Birnhack & Niva. "The Invisible Handshake: The Reemergence of the State in the Digital Environment." 2003.

McCullagh, Declan. "Terrorism Invoked in ISP Snooping Proposal." 30 May 2006. CNET NEWS.COM. <http://news.com.com/2100-1028\_3-6078229.html>.

Simpson, Gemma. "Google Scores Lowest in Privacy Rankings." 12 June 2007. ZDNET. <http://news.zdnet.co.uk/internet/0,1000000097,39287492,00.htm.>.

Taipale, K.A. "Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data." 2003.

Tene, Omer. "What Google Knows: Privacy and Internet Search Engines." Selected works of Omer Tene. <http://works.bepress.com/omer\_tene/2/>.

Young, Alyson L. "Information Revelation and Internet Privacy Concerns on Social Network Sites: A Case Study of Facebook." The University of Western Ontario, n.d.

1. Google Privacy Policy, http://www.google.com/intl/en/privacypolicy.html#information. *See also* Google Privacy FAQ, http://www.google.com/intl/en/privacy\_faq.html. [↑](#footnote-ref-1)
2. *See* Google.com, Corporate Information, Our Philosophy, Never Settle for the Best, http://www.google.com/corporate/tenthings.html. [↑](#footnote-ref-2)