"*I Know Who You Are and I Saw What You Did* shows how the way society deals with the online world needs to be rethought, as the current methods make every one of us a potential victim."
—*New York Post*

I KNOW WHO YOU ARE AND I SAW WHAT YOU DID

Social Networks and the Death of Privacy

LORI ANDREWS

2

George Orwell . . . Meet Mark Zuckerberg

On a Sunday morning, I fire up my laptop and compose a memo to my co-counsel about a pro bono case we are considering filing against a biotechnology company. I attach it to an email and send it to him, carefully writing, "Confidential—Legal Mail" in the subject line and putting a few key ideas in the text of the email. Then I log on to the Southwest Airlines site, enter my credit card information, and buy a ticket for Florida. I enter a governmental website, run by the Florida Fish and Wildlife Conservation Commission, and type in my Social Security number to obtain a fishing license. I realize I'll be away on my sister's birthday and send her some books from Amazon. I check my emails and click through to a website that lists job openings for university professors. One is in a town I haven't heard of, so I Google it to find out if it will be urban enough for me. The town's name brings up a link to a local newspaper article about a poisoning and I save that information to my hard drive, thinking I might use it in the next mystery book I write. I read an email from my doctor telling me she changed my prescription electronically and the new drug is waiting for me at my neighborhood CVS. Before leaving the house to pick it up, I log on to Facebook to contact friends in Florida and let them know when I'll arrive. Elsewhere on my Facebook page, I check my news feed and indicate I liked the movie I saw the previous night. Someone has tagged me in a Halloween photo from years ago, when I was a Yale undergrad. I am wearing a belly dancer's costume and I am with someone dressed like a bottle of Imperial Single Malt Scotch. I untag myself from the photo. If I do interview for a new job, I don't want someone to say to me, "Well, Ruth Bader Ginsburg would never have shown her navel."

All in all, I feel good about the security of my morning's travels across the Web. I haven't responded to any wealthy widows seeking my legal help for their $50 million estates, nor to emails purportedly from friends whose wallets and passports were stolen in London. I haven't given my credit card to anyone with a sketchy foreign email address who offers me an iPad for $30, nor have I opened the missive that tells me I've exceeded my email limit. I've only dealt with websites I trust.

But every action I've taken has been surreptitiously chronicled and analyzed by data aggregators, who then sell the information to companies, including perhaps the one I am contemplating suing. And not only have I not been informed about this invasion of my privacy and security, there's almost nothing I can do about it.

That stunning fact is completely at odds with the offline world. I care deeply about the type of information I've entered. I wouldn't leave my Social Security number or my credit card number lying on my desk at work where someone could copy it—nor would I send that information on a postcard through the mail. I wouldn't broadcast my medical condition or my desire to find a new job to the world. But that information about me is bought and sold daily by corporations that deal with data aggregators.

If someone broke into my home and copied my documents, he'd be guilty of trespass and invasion of privacy. If the cops wanted to wiretap my conversation, they'd need a warrant. But without our knowledge or consent, virtually every entry we make on a social network or other website is surreptitiously being tracked and assessed. The information is just as sensitive. The harms are just as real. But the law is not as protective.

The guiding force behind this enormous theft of private information is behavioral advertising. The covert collection of personal information is an exploding industry, fueled in part by the lust of advertisers for personal data about people's habits and desires. "Online behavioral advertising," notes the Federal Trade Commission, "involves the tracking of consumers' online activities in order to deliver tailored advertising. The practice, which is typically invisible to consumers, allows businesses to align their ads more closely to the inferred interests of their audience."[1] But the unregulated amassing of personal information about people has also been used in ways that cause them harm.

Behavioral advertising was used by 85% of ad agencies in 2010.[2] They're drawn to it because it works—63% of ad agencies say targeted ads increased their revenue, with 30% of agencies reporting that behavioral advertising increased their revenue by $500,000 or more. In 2010, internet advertising revenues exceeded that of newspapers by $3.2 billion.[3] During the first quarter of 2010, internet users in the United States received 1.1 trillion display ads, which cost the ad sponsors about $2.7 billion.[4]

"It's a digital data vacuum cleaner on steroids, that's what the online ad industry has created," Jeff Chester, executive director of the Center for Digital Democracy, told *The New York Times*. "They're tracking where your mouse is on the page, what you put in your shopping cart, what you don't buy. A very sophisticated commercial surveillance system has been put in place."[5]

It's through data aggregation that Facebook makes its money. Facebook sits on a mountain of information worth a fortune. Facebook was valued at $42 billion in August 2012.[6] Currently the company generates most of its revenue by acting as an intermediary between advertisers and its database of users' personal information. Facebook will use information about my status, likes and dislikes, and the

recent post about my travel plans to update its digital portrait of me. When an airline or outdoor clothing company pays Facebook to post an ad for traveling adults, Facebook will use its new information about me to post the ad on my Facebook page. This commercialization of my private data—the information I think I'm only posting to friends—is the reason Facebook earned an estimated $1.86 billion in 2010 from the display ads, 90% of its total revenue, and was expected to bring in $4.05 billion in advertising revenue the following year.[7]

Facebook uses its citizens' demographic information, interests, likes, friends, websites frequented, and even contact information as the foundation of its advertising platform. Facebook encourages users to disclose more information about themselves through "very powerful game-like mechanisms to reward disclosure," said media activist Cory Doctorow, co-editor of Boing Boing.[8] Doctorow compares Facebook's mechanisms to the famous Skinner box used in psychology experiments.[9] But instead of a lab rat rewarded with a food pellet each time it pushes a lever in the box, a Facebook user is rewarded with "likes" and attention from friends and family each time that person posts more information.

"And this is not there because Facebook thinks that disclosing information is good for you necessarily," says Doctorow. "It's in service to a business model that cashes in on the precious material of our social lives and trades it for pennies."

But the collection and marketing of personal information are far more insidious, and profitable, than just the actions of Facebook. Mark Zuckerberg's brainchild makes up only 14.6% of the behavioral advertising market. And some of the other advertisers use tactics that make Zuckerberg's seem tame. Every single action I undertook that Sunday morning was potentially seized by a data aggregator through some means or another. In California, consumers sued the company NebuAd, which contracted with 26 internet service providers, including Delaware's Cable One, New York's Bresnan Communications, and Texas's CenturyTel, to install NebuAd's hardware on those internet service providers' networks without ISP users' consent.[10] The hardware allowed NebuAd to use deep packet inspection—a mechanism to intercept and copy all the online transmissions of the ISPs' subscribers and transmit them to NebuAd's headquarters.[11] All of them.

Everything you post on a social network or other website is being digested, analyzed, and monetized. In essence, a second self—a virtual interpretation of you—is being created from the detritus of your life that exists on the Web. Increasingly, key decisions about you are based on that distorted image of you. Whether you get a mortgage, a kidney, a lover, or a job may be determined by your digital alter ego rather than by you.

In the late 1960s, sociologist John McKnight, then Director of the Midwest Office of the U.S. Commission on Civil Rights,[12] coined the term "redlining" to describe the failure of banks, supermarkets, insurers, and other institutions to offer their services in inner city neighborhoods.[13] The term came from the practice of banks, which drew a red line on a map to indicate where they wouldn't invest.[14] But

use of the term expanded to cover a wide array of racially discriminatory practices in general, such as not offering home loans to African Americans, even if they were wealthy or middle class.

Now the map used in redlining is not a geographic map but the map of your travels across the Web. A new term, "weblining," covers the practice of denying certain opportunities to people due to observations about their digital selves. Sometimes redlining and weblining overlap, such as when a website uses zip code information from a social network or an online purchase elsewhere to deny a person an opportunity or charge him a higher interest rate.

"There's an anti-democratic nuance to all of this," says New York University sociologist Marshall Blonsky. "If I am Weblined and judged to be of minimal value, I will never have the products and services channeled to me—or the economic opportunities—that flow to others over the Net."[15]

Data aggregation is big business. The behemoth in the industry, Acxiom, has details on everything from your Social Security number and finances to your online habits.[16] Its former CEO, John Meyer, described it as "the biggest company you've never heard of."[17] Rapleaf is another data aggregator that combines online data, including usernames and social networks, and offline data from public records.[18] One of its competitors, ChoicePoint, has acquired more than 70 smaller database companies and will sell clients one file that contains an individual's credit report, motor vehicle history, police files, property records, court records, birth and death certificates, and marriage and divorce decrees.[19] Yet ChoicePoint didn't do a great job of keeping that information secure. In 2005, identity thieves who submitted false applications to ChoicePoint claiming to be small businesses were given access to ChoicePoint's database that contained financial records of more than 163,000 consumers.[20] The Federal Trade Commission attributed the security breach to a lack of proper security and record handling procedures and, as part of a settlement with ChoicePoint, required the company to implement a comprehensive information security program and to pay $10 million in civil penalties and $5 million to reimburse the consumers affected by the identity theft.[21] That same year, hackers targeted LexisNexis (an aggregator which later bought ChoicePoint for $4.1 billion in cash), and accessed the personal information of 310,000 customers.[22]

Weblining goes further than traditional redlining. Sometimes an individual's credit card limit is lowered, midcourse, based on data from aggregators, even when the cardholder has done nothing wrong. Kevin Johnson, a condo owner and businessman, held an American Express card with a $10,800 limit. When he returned from his honeymoon, he found that the limit had been lowered to $3,800. The switch was not based on anything Kevin had done but on aggregate data. A letter from the company told him: "Other customers who have used their card at establishments where you recently shopped have a poor repayment history with American Express."[23]

Not only does weblining affect what opportunities are offered to you (in the

form of advertisements, discounts, and credit lines), it also affects the types of information you see. When you open Yahoo! News or go to other news websites, you get a personalized set of articles, different from your spouse's or neighbor's. That may sound like a good thing, but you may be losing out on the big picture. With the physical version of *The New York Times*, you'd at least see the headlines about what was going on in the world, even if you were skimming the paper to get to the movie reviews. But world news may disappear entirely from your browser if you have indicated an interest in something else. Ever since I clicked on a story about the royal wedding, the world news stories I used to receive when I logged on to my email have been replaced by celebrity breakup and fashion stories. But if we are all reading a different, narrow range of articles, how can we participate in a civic democracy?

"Ultimately, democracy works only if we citizens are capable of thinking beyond our narrow self-interest. But to do so, we need a shared view of the world we cohabit," says Eli Pariser in *The Filter Bubble: What the Internet Is Hiding from You*. Pariser explains that the internet initially seemed like the perfect tool for democracy. But now, he points out, "Personalization has given us something very different: a public sphere sorted and manipulated by algorithms, fragmented by design, and hostile to dialogue."[24]

Most people have no idea how much information is collected surreptitiously about them from social networks and other websites. When asked about behavioral advertising, only half of the participants in a 2010 study believed that it was a common practice.[25] One respondent said, "Behavioral advertising sounds like something my paranoid friend would dream up, but not something that would ever really occur in real life."

People have a misplaced trust that what they post is private. A Consumer Reports poll found that "61% of Americans are confident that what they do online is private and not shared without their permission" and that "57% incorrectly believe that companies must identify themselves and indicate why they are collecting data and whether they intend to share it with other organizations."[26]

When people realize that websites and advertising companies are collecting extensive information about them, many want legal change. A telephone survey found that 66% of adult Americans opposed being targeted by behavioral advertising and are troubled by the technologies used to enable it.[27] Also, 68% of Americans opposed being "followed" on the Web and 70% of Americans supported the idea of requiring hefty fines to be paid by a company that collects or uses someone's information without his or her consent. Most people—92%—believe that websites and advertising companies should be required to delete all information stored about an individual if requested to do so.

Your ability to protect yourself against unwanted data collection depends largely on the technique being used to acquire information. With some methods, companies use your own computer against you by instructing your internet browser to store information on your computer's hard drive that data aggregators can use

to track your movement online and build a profile of your online behaviors. Other methods tap the information as it travels from your computer to the recipient's website or email address. (See "Web Tracking Chart.")

The collection of information from websites and social networks began modestly enough. Social networks asked you if you'd like to have your password stored. Websites like Amazon.com began to keep track of your purchases on their sites to make recommendations and to allow you the convenience of not re-entering a password or credit card number each time you visit the site. Now tracking technologies with names like cookies, Flash cookies, web beacons, deep packet inspection, data scraping, and search queries allow advertisers to create a picture of you by noting what you look at, look up, and buy across the internet. Sometimes this information is even linked to offline purchases and activities you engage in.

Until I started writing this book, I had no idea that Comcast, my internet service provider, installed more than a hundred tracking tools.[28] Dictionary.com (one of my favorite websites, which I use more often than Facebook) installed 234 tracking tools on a user's computer without permission, only 11 from Dictionary.com itself and 223 from companies that track internet users.[29] The vast majority of these tools, according to a report by *The Wall Street Journal*, did not allow users to decline tracking. Among the 50 top sites assessed in this study by *The Wall Street Journal*, Dictionary.com "ranked highest in exposing users to potentially aggressive surveillance."

Increasingly ingenious and troubling technologies are used to learn ever more about you. Two apps on the iPhone and Android devices—Color and Shopkick—activate your phone's microphone and camera to collect background sound and light patterns from your location, be it a bar, your office, or your home. Using the same type of program that allows your iPhone to name a song based on just a few notes, Color makes assessments about your location to alert you if other people in your social network are nearby and Shopkick assesses if the store you've entered has a bargain to offer you. Silicon Valley blogger Mike Elgan points out the wealth of information marketers can collect about you through these phone apps: "Your gender, and the gender of people you talk to; your approximate age, and the ages of the people you talk to; what time you go to bed, and what time you wake up; what you watch on TV and listen to on the radio; how much of your time you spend alone, and how much with others; whether you live in a big city or a small town; what form of transportation you use to get to work."[30]

Browser cookies can be used by data aggregators to collect user IDs, user-selected preferences, demographics, purchasing histories, creditworthiness, log-in names, Social Security numbers, credit card numbers, phone numbers, and addresses.[31] How do they work? When a user types the web address (known as a URL) of a social network or website into a browser or clicks on a link for a website—as I did when I ordered books on Amazon—the browser contacts the website's server and requests the page.[32] The website's server then sends the requested web page to the browser. The website server treats each request as if it were the first request

it had received from the user—the website server has no memory.[33] But when the website server places a small line of text—known as a cookie—on your computer, it can keep track of your subsequent visits to its web pages and actions you took on its website (for example, the title of the books you ordered on Amazon, as well as those you looked at but didn't order).[34] That information can be used to create personalized ads to sell you additional products in the future (such as other books of the genre you ordered).

A cookie can also be placed on a user's hard drive by a third-party advertiser. By 2001, the data aggregator DoubleClick had convinced 11,000 websites (including 1,500 of the most highly trafficked websites, such as AltaVista, *U.S. News and World Report* online, *The Wall Street Journal*, theglobe.com, NBC, *Reader's Digest*, and Bloomberg) to allow it to place cookies on their users' computers.[35] DoubleClick could then collect and aggregate data about what the user did on any of those 11,000 websites. DoubleClick used the information collected for behavioral advertising so their clients could decide which banners would be displayed when a particular person visited the Web. Here is an example of a DoubleClick cookie: id 80000008xxxxxxb doubleclick.net/ 0 1468938752 31583413 158986260829410552.*[36] And this is an example of a cookie from Hotmail in the Internet Explorer browser: HMP1|1|hotmail.msn.com/|0|1715191808|32107852|3511491552|29421613|*|.[37]

A web beacon (also called a web bug, action tag, pixel tag, or clear GIF) can be used as an alternative means to compile information about an internet user. A web beacon is a small graphic image that is usually transparent (and therefore invisible to the user) and no larger than one pixel by one pixel that is placed on a website or in an email.[38] When an internet user visits a web page or opens an email containing a web beacon, the code of the web page or email instructs the computer to contact another server to download the web beacon.[39] This server is operated either by the owner of the website or by a third party that has permission to place the web beacon on the owner's website.[40] When the computer contacts the server to retrieve the small graphic image, the server generates a file about characteristics of the user, such as the internet protocol address (the unique address of the requesting computer), the web address of the page the person is viewing, the time the web beacon was loaded, and the type of browser that retrieved the web beacon.[41] This is an example of a DoubleClick web beacon hidden in the HTML code of Quicken: <img src="http://ad.doubleclick.net/ad/pixel.quicken/NEW" width=1height=1 border=0>.[42]

Frequently web beacons and cookies are used in tandem. A web beacon can be used to deliver a browser cookie to the user's computer.[43] Through this method, a web server can recognize a browser across a number of domains and sites, permitting data aggregators to capture a user's web activity.[44]

Web beacons are everywhere. In a 2009 University of California at Berkeley study, each of the 50 most visited websites contained at least one web beacon, while most sites had several and some sites had as many as a hundred.[45] And some

tracking companies have a wide scope of coverage. Google and its subsidiaries, for example, had web beacons on 92 of the top 100 websites.

Data aggregators also gather information via Flash cookies, which have been described as a "normal browser cookie on steroids."[46] Adobe Flash Player is software for viewing certain videos, animations, web apps, games, text, and images in internet browsers.[47] To support this, the Adobe Flash Player has its own storage system. Websites containing Flash applications can store information on an individual's hard drive. The data storage file, known as a Flash cookie, is used by websites to keep track of the user's preferences, such as the volume setting for a particular Flash application. But, just like browser cookies, Flash cookies have been co-opted by advertising networks and data aggregators to collect and store information about the browsing habits of internet users. And Flash cookies offer advertisers and data aggregators advantages over browser cookies, since they can store up to 100 kilobytes of information, while browser cookies can store only 4 kilobytes.[48] Flash cookies are also harder to get rid of than normal cookies. Erasing browser cookies, clearing browser history, erasing the cache, deleting private data within the browser, or changing the browser to "private browsing," which can remove or disable browser cookies, sometimes does not affect the Flash cookies.[49] Plus, deleted browser cookies can be "raised from the dead" by Flash cookies, creating "zombie" cookies.[50] A website server will place both browser and Flash cookies on a user's computer, and the Flash cookie will store the browser cookie's unique cookie ID. When the Flash cookie is activated, it will check for the existence of the browser cookie, and if the browser cookie does not exist because the user deleted it, the Flash cookie creates and installs another one.[51]

The most aggressive and problematic technology used for data aggregation and behavioral marketing is deep packet inspection. This technology allows internet service providers (ISPs) or third parties to collect and analyze the internet transmissions of an ISP's users.[52] Transmissions sent on the internet are broken into digital packets, each of which contains only a portion of the original transmission but all of which contain the internet protocol addresses of the sender and the recipient and an indication of that packet's place in the complete transmission. These packets are transmitted from router to router across the internet to their destination. Since some routers might be busy at a particular moment, sometimes packets are sent along different routes to the same destination.

As one judge explained it, "If a computer in New York sent a document to one in Boston, some packets might travel through routers and cables directly up the east coast while other packets might be sent by way of Seattle or Denver, due to momentary congestion on the east coast routes."[53]

Deep packet inspection by the internet providers themselves has a number of legitimate uses: detecting network attacks, managing network congestion, and charging different prices for different internet services.[54] But some behavioral marketing firms contract with ISPs to spy on—and copy—what users are sending.[55] The data aggregators place a tap on the ISP's equipment and collect and inspect

all the packets of information sent out by users. This is a massive amount of data, including every email you send, every website you browse, voice-over-internet-protocol (VOIP) phone calls (such as through Skype), peer-to-peer file transfers, and online gaming. In her statement to the House Subcommittee on Telecommunications and the Internet in July 2008, Alissa Cooper, chief computer scientist for the Center for Democracy & Technology,[56] analogized deep packet inspection to a post office opening and reading a letter before it is sent.[57]

The data aggregator receives data packets from a person's transmissions and analyzes the content of the packets to create a profile of the person's online behaviors and interests. The aggregator can then sell the information and analyses to others, including advertisers who create targeted ads based on people's behavioral profiles.

When I did my Sunday morning business on social networks and websites, I had no intention to let others peek at—let alone sell—the information that could be gleaned about me from what I wrote, bought, sent, or viewed. "In part because the Internet was developed around the end-to-end principle, consumers have come to expect that their Internet communications pass through the network without being snooped on the way," says Cooper. "Deep packet inspection dramatically alters this landscape by providing an ISP or its partners with the ability to inspect consumer communications en route. Thus, deploying a DPI system likely defies the expectations consumers have built up over time."[58]

Even the games you play and the apps you use on Facebook can collect and transmit personal information about you. In 2007, Facebook launched a platform that let software developers build applications that run on the site. By 2011, there were more than 550,000 apps, and those apps have become an industry, with social games, the biggest category of apps, having a projected revenue of $1.2 billion annually.[59] Facebook reported in 2010 that 70% of its users run at least one app each month.[60]

A 2010 investigation by *The Wall Street Journal* found that many of the most popular applications on Facebook were transmitting identifying information about users and their friends to advertisers and internet tracking companies, which is a violation of Facebook's privacy policy.[61] *The Wall Street Journal* analyzed the ten most popular Facebook apps, including Zynga's FarmVille, with 59 million users, and Zynga's Mafia Wars, with 21.9 million users, and found that they were transmitting Facebook user IDs to data aggregators. When a data aggregator has a Facebook ID, it can access any public information on a person's Facebook page (which could include the person's name, age, residence, occupation, and photos). The Zynga applications were sharing Facebook users' IDs with the internet tracking company Rapleaf, which then added the information to its own database of internet users for enhanced behavioral advertising.[62]

Rather than focusing on an individual's interaction with a website, some data aggregators use a method known as "scraping" to extract all the data that anyone has posted on a particular website, analyze it, and sell it. Web scrapers copy information from websites through specially coded software.[63] These software programs

are also referred to as web robots, crawlers, spiders, or screen-scrapers. Scrapers are designed to search through the HTML code that makes up a website and extract desired information. If a certain website includes a discussion by new moms (or by people considering buying cars), the data scraper can sell that information and the people's email addresses or IP addresses to advertisers who want to target ads to those types of consumers.

Web scrapers "are capable of making thousands of database searches per minute, far exceeding what a human user of a website could accomplish," says attorney Sean O'Reilly, who previously worked in the software industry. "Web vendors have a difficult time detecting a difference between consumers accessing this information for their own benefit, and aggregators accessing the information to return to their own databases."[64]

Search engines such as Google, Yahoo!, and Bing also collect, store, and analyze information about individual users through their search queries. Search engines maintain "server logs," which, according to Google's Privacy Policy, include 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."[65] Microsoft's search engine, Bing, adds that it also "will attempt to derive your approximate location based on your IP address."[66] Search engines use this information to optimize their search algorithms and to record an individual's preferences.[67] Though Google uses these logs for fraud prevention and to improve search results, it also analyzes the logs to generate more revenue through targeted advertising.[68] Yahoo! also uses this information to personalize advertising and page content. Yahoo! acknowledges that it also allows other companies to display ads on its pages and those ads may "set and access cookies on your computer" that are not subject to Yahoo!'s privacy policy.[69]

In 2006, AOL made public 20 million queries entered into its search engine from 658,000 users on its website research.aol.com.[70] AOL's release contained all of those users' searches over a three-month period and detailed whether they clicked on a result, what the result was, and where it was in the list of results.[71] An AOL researcher, Abdur Chowdhury, explained the release of the queries as an effort to facilitate "closer collaboration between AOL and anyone with a desire to work on interesting problems."[72] But the project ended up breaching people's privacy. In some instances, people could be identified through the types of searches they undertook.

A quick look at some of the leaked AOL search logs makes it easy to imagine how damaging a search log can be when linked to a party in a criminal, civil, or divorce case.

User 11574916:
cocaine in urine
asian mail order brides

states reciprocity with florida
florida dui laws
extradtion from new york to florida
mail order brides from largos
will one be extradited for a dui
cooking jobs in french quarter new orleans
will i be extradited from ny to fl on a dui charge

User 336865:
sexy pregnant ladies naked
nudist
sexy feet
child rape stories
tamagotchi town.com
preteen sex stories
illegal child porn
incest stories
10 year old nude pics
preteen nude models
illegel anime porn
yu-gi-oh

User 59920:
cats skinned in fort lupton co
cats killed in fort lupton co
jonbenets autopsy photos
crime scene photos of the crawl space and duffle bag in ramseys house
sexy bathing suits
what a neck looks like after its been strangled
pictures what a neck looks like after it was strangled
pictures of murder victims that have been strangled
pictures of murder by strangulation
knitting stitches
what jonbenet would look like today
new jersey park police
jonbenet in her casket
ransom note in the movie obsession what did it read
movie ransom notes
scouting knots
manila rope and its uses
brown paper bags cops use for evidence
rope to use to hog tie someone
body transport boulder colorado

User 1515830:
chai tea calories
calories in bananas
aftermath of incest
how to tell your family you're a victim of incest
pottery barn
curtains
surgical help for depression
oakland raiders comforter set
can you adopt after a suicide attempt
who is not allowed to adopt
i hate men
medication to enhance female desire
jobs in denver colorado
teaching positions in denver colorado
how long will the swelling last after my tummy tuck
divorce laws in ohio
free remote keyloggers
baked macaroni and cheese with sour cream
how to deal with anger
teaching jobs with the denver school system
marriage counseling tips
anti psychotic drugs[73]

Your web searches provide data on which you can be judged, erroneously or not. If you've looked up the side effects of antidepressants, that information might be used against you by an employer or a college admissions officer. Your search for a divorce lawyer, advice about green cards, or information about sexually transmitted diseases might also be used in ways that harm you.

Your second self on the Web is likely a distortion of your offline self. The person whose leaked AOL searches related to extradition might have been writing a mystery, rather than covering up a crime. The woman who was seeking information on AOL about incest might have been trying to help a friend, rather than dealing with her own troubled past.

When AOL released the supposedly anonymous queries, it was easy for reporters from *The New York Times* to identify Thelma Arnold as searcher 4417749 due to her searches for other Arnolds and her searches about Lilburn, Georgia.[74] After discussing her queries for 60-year-old single men, queries about her three dogs, and queries researching her friends' ailments, Thelma said, "My goodness, it's my whole personal life. I had no idea somebody was looking over my shoulder."[75]

But "in user search query logs, what you see is not always what you get," notes Omer Tene, a professor at a law school in Rishon Le Zion, Israel. Anyone who had access to Thelma Arnold's logs saw searches for "hand tremors," "nicotine effects

on the body," "dry mouth," "bipolar," and "single dances in Atlanta." However, those were searches Thelma conducted for others and do not paint an accurate picture of her life or health.[76]

The attributes of your digital doppelgänger may have more influence on what opportunities you receive than any of your offline characteristics. Rather than expanding opportunities for you, the targeted ads that you see may actually deny you certain benefits. You might be shown a credit card with a lower credit limit, not because of your credit history but because of your race, sex, zip code, or the types of websites you visit. As a consequence of weblining, the information collected by data aggregators is often sold to the public at large (through websites such as Spokeo) and might later hamper your efforts to get a job, qualify for a loan, adopt a child, or fight for your rights in a criminal trial.

As behavioral advertisers increasingly dictate a person's online and offline experiences, stereotyped characterizations may become self-fulfilling. Rather than reflecting reality, behavioral analysis may inevitably define it. When young people from "poor" zip codes are bombarded with advertisements for trade schools, they may be more likely than their peers to forgo college. And when women are routinely shown articles about cooking and celebrities, rather than stock market trends, they will likely disclaim any financial savvy in the future. Behavioral advertisers are drawing new redlines, refusing to grant people the tools necessary to escape the roles that society expects they play. Our digital doppelgängers are directing our futures and the future of society.

Some social network users feel that access to their personal data is a small price to pay for the ability to use Facebook and other websites without charge. Other people, though, do not want to face discrimination based on their second self and want to use technological and legal measures to assert control over their own data. Still others feel that information about them should be considered to be their property and if anyone is going to make money by selling that data, it should be them. Yet without a Social Network Constitution, individual choices go unrecognized as the networks and data aggregators call the shots.

A shift away from third parties piecing together and shaping our second selves is imperative to avoid predetermined fates. We must be given an opportunity to create our own alter egos and paint a unique, personal self-portrait. A Social Network Constitution will help us do just that. It can restore power to the people and open up the possibility for individuals to once again explore their identities and determine their fates.

WEB TRACKING CHART

	Deep-Packet Inspection	Scraping	Flash Cookies	Browser Cookies	Search Engines	Remotely Installed Keylogger
Sensitive information submitted through web forms (e.g., credit card info, Social Security number, passwords)	**Yes**	**No**	**Yes**	**Yes**	**No**	**Yes**
Skype calls (to whom, for how long)	**Yes***	**No**	**No**	**No**	**No**	**No**
Websites visited in a session	**Yes**	**No**	**Yes**	**Yes**	**No**	**No**
How long you've stayed on a page	**Yes**	**No**	**Yes**	**Yes**	**No**	**No**
Your IP address when you access a page	**Yes**	**No**	**Yes**	**Yes**	**No**	**No**
Facebook postings (public)	**Yes**	**Yes**	**No**	**No**	**Yes**	**Yes**
Facebook postings (private)	**Yes**	**Yes†**	**No**	**No**	**No**	**Yes**
Contents of private forum posts (e.g., posts on PatientsLikeMe)	**Yes**	**Yes†**	**No**	**No**	**No**	**Yes**
Content of sent emails	**Yes**	**No**	**No**	**No**	**No**	**Yes**
Content of attachments in sent emails	**Yes**	**No**	**No**	**No**	**No**	**No**
Ticket purchase info on airline site	**Yes**	**No**	**Yes**	**Yes**	**No**	**No**
Info submitted to government site to obtain license	**Yes**	**No**	**Yes**	**Yes**	**No**	**Yes**
Browsing and purchasing activity on Amazon.com	**Yes**	**No**	**Yes**	**Yes**	**No**	**No**
Clicks through to a website via email link	**Yes**	**No**	**Yes**	**Yes**	**No**	**No**
Search query about a town	**Yes**	**No**	**Yes**	**Yes**	**Yes**	**Yes**

	Deep-Packet Inspection	Scraping	Flash Cookies	Browser Cookies	Search Engines	Remotely Installed Keylogger
Download of a newspaper article (plus possibly the title from the URL)	**Yes**	**No**	**Yes**	**Yes**	**No**	**No**
Doctor email changing prescription electronically	**Yes**	**No**	**No**	**No**	**No**	**No**
Facebook activity (that doesn't require typing)	**Yes**	**No**	**Yes**	**Yes**	**No**	**No**
Untagging personal photo	**Yes**	**No**[§]	**No**	**No**	**No**	**No**

*However, even if the interception of voice traffic is technically possible, the compressed data will likely be encrypted.

†Yes, though collectable data is limited to accounts with which the scraper's account is friends.

‡Having an account is necessary to access private forums.

§Prior to untagging, scrapers with Facebook accounts that can view the image will also be able to collect the data linking you to the image.

Thanks to Cynthia Sun for the preparation of this chart.