

Hi, my name is Sherri Davidoff. I'm a computer forensic investigator and a network security professional. One of my jobs is to assess the security of my clients' networks. Over the past decade, I have had the opportunity to see inside the computer networks of many different types of organizations, including health care institutions, government agencies, financial institutions, retailers, telecommunications companies, and more. I've had the opportunity to see first hand the types of information these organizations collect, and how well they manage-- or don't manage-- their security. From a personal perspective, what I have seen is frightening. I am here today to tell you a little bit about it.

When you go to the store, and you buy a box of cold medicine, or a book, or ammunition, and you pay with a card, that information is recorded. The credit card issuer tracks the location, date, time and type of each purchase. The store itself may track very granular information about your purchases, such as the names of the movies you buy or the caliber, type and quantity of ammunition you purchased.

Your purchase histories, including what you purchased, where and when, is then sold to marketers, insurance companies, the federal government, pretty much anyone who is willing to pay for it.

This has become a huge industry.

When you walk around on the street, your cell phone tracks you everywhere you go. The FCC required that all cell phones have highly granular GPS tracking capabilities, for the purposes of emergency 911 calls. However, software writers and mobile carriers use this to keep detailed location histories of YOU which they use for their own profit. Software writers who create apps on your phone can record your location as you travel, and sell records of your location history to whomever they want! When you visit someone's house, when you go to the bar, you can be tracked and your location records can be sold to marketers, insurance companies, the federal government, anybody.

Your medical prescription information is not private the way you think it is. Prescription information has been bought and sold for decades. In recent years, the federal government has been passing stronger laws regarding medical data privacy. Unfortunately, the budgets of health care organizations are often very stretched, and they often do not have the resources to comply, or to properly secure sensitive medical information. I have seen this countless times with my own two eyes. In Montana, medical information is not included as "personal information" under our state data breach notification law, so under state law, data holders are not required to notify you if your medical information is stolen.

Now that health information is becoming electronic, companies like Google are offering medical record storage and management services. These companies are NOT health care providers and they are NOT required to abide by HIPAA, which limits how medical information can be distributed.

There are many companies that track your web browsing habits online. When you visit a web site or type information into your computer, your web browsing history is tracked and sold. The words you type into searches are tracked and sold. This can include health information, financial information, your interests and habits. If you think it's anonymous, guess again. Have you ever typed your own name or address into your computer? Have you ever bought anything online with your credit card? Have you ever entered your email address or a blog username linked to your real name? There are companies which specialize in figuring out your real name and matching that to your web browsing history, which is frequently and invisibly tracked by third parties.

There are also companies that collect your web browsing history, and tie that into your purchase histories (from credit cards or stores), motor vehicle records, medical information, and much more. These detailed personal "dossiers" about YOU are sold to advertisers, financial institutions, governments and more for profit. Companies can use them for price discrimination, marketing different products and prices to you based on the information they have. Banks could deny you loans based on your web surfing history. This information is extremely valuable, and extremely dangerous.

You would think that companies carefully secure this extremely personal information, but most of the time, they don't. If your credit card number gets stolen, and nobody finds out about it, is there any cost to the merchant? If your health information is stolen, and the company that was keeping it never tells anyone, will they suffer any loss themselves? There's little incentive for the companies trading this personal information to invest a lot of resources in keeping your most private data secure. Instead, they just use it, sell it, and try to minimize their own costs. As a result, the more your personal information is bought and sold, the higher your risk for identity theft.

I am proud to be a Montanan. I am proud to live in a state where citizens have a Constitutional right to privacy, and are willing to stand up for it. Over the past decade, technology has moved so quickly that the law hasn't been able to keep up.

As a result, Montana citizens are being constantly exploited. Our movements are being tracked. Our purchases are being recorded and sold. Our activities are being watched. Most of the time, this happens invisibly, without our knowledge and without our consent.

I believe that this is directly opposite of what our constitutional framers intended, and what most Montana citizens would want. We don't want to be bought and sold. We value our freedom here, and our privacy.

It is time for us to catch up with technology, to conduct a study, and to examine the ways that we can protect Montana citizens, while still balancing the needs of our state and local governments, and our business community.

# Cell Phone Tracking

The Wall Street Journal - WSJ Blogs

"What They Know - Mobile"

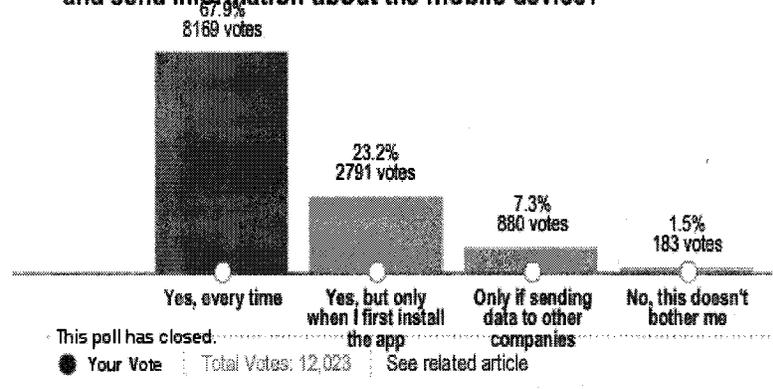
<http://blogs.wsj.com/wtk-mobile/>

Marketers are tracking smartphone users through "apps" - games and other software on their phones. Some apps collect information including location, unique serial-number-like identifiers for the phone, and personal details such as age and sex. Apps routinely send the information to marketing companies that use it to compile dossiers on phone users. As part of the What They Know investigative series into data privacy, the Journal analyzed the data collected and shared by 101 popular apps on iPhone and Android phones (including the Journal's own iPhone app). This interactive database shows the behavior of these apps, and describes what each app told users about the information it gathered.



**Identity  
Location  
Contacts**

Do you think apps should tell you when they collect and send information about the mobile device?



## THE WALL STREET JOURNAL

App name	iPhone		Android			
	Username, Password	Contacts	Age, Gender	Location	Phone ID	Phone number
0.03 Seconds Pro	Does not transmit data	Does not transmit data	Does not transmit data	Does not transmit data	Transmits data to third parties	Does not transmit data
Age My Face	Does not transmit data	Does not transmit data	Does not transmit data	Does not transmit data	Transmits data to third parties	Does not transmit data
Angry Birds	Transmits data to third parties	Does not transmit data	Does not transmit data	Transmits data to third parties	Transmits data to third parties	Does not transmit data
Angry Birds Lite	Transmits data to third parties	Does not transmit data	Does not transmit data	Transmits data to third parties	Transmits data to third parties	Does not transmit data
Aurora Feint II: Lite	Transmits data to app owner	Does not transmit data	Does not transmit data	Transmits data to third parties	Transmits data to third parties	Does not transmit data
Barcode Scanner (BahnTech)	Does not transmit data	Does not transmit data	Does not transmit data	Does not transmit data	Transmits data to third parties	Does not transmit data
Bejeweled 2	Transmits data to third parties	Does not transmit data	Does not transmit data	Does not transmit data	Does not transmit data	Transmits data to third parties
Best Alarm Clock: Free	Does not transmit data	Does not transmit data	Does not transmit data	Transmits data to third parties	Transmits data to third parties	Does not transmit data
Bible App (LifeChurch.tv)	Does not transmit data	Does not transmit data	Does not transmit data	Transmits data to third parties	Transmits data to third parties	Does not transmit data
Bump	Does not transmit data	Does not transmit data	Does not transmit data	Does not transmit data	Does not transmit data	Does not transmit data
CBS News	Does not transmit data	Does not transmit data	Does not transmit data	Transmits data to third parties	Transmits data to third parties	Does not transmit data
0.03 Seconds	Does not transmit data	Does not transmit data	Does not transmit data	Does not transmit data	Transmits data to third parties	Does not transmit data
Dictionary.com	Does not transmit data	Does not transmit data	Does not transmit data	Transmits data to third parties	Transmits data to third parties	Does not transmit data
Doodle Jump	Transmits data to third parties	Does not transmit data	Does not transmit data	Does not transmit data	Transmits data to app owner	Does not transmit data

## "The Tracking Ecosystem" - The Wall Street Journal

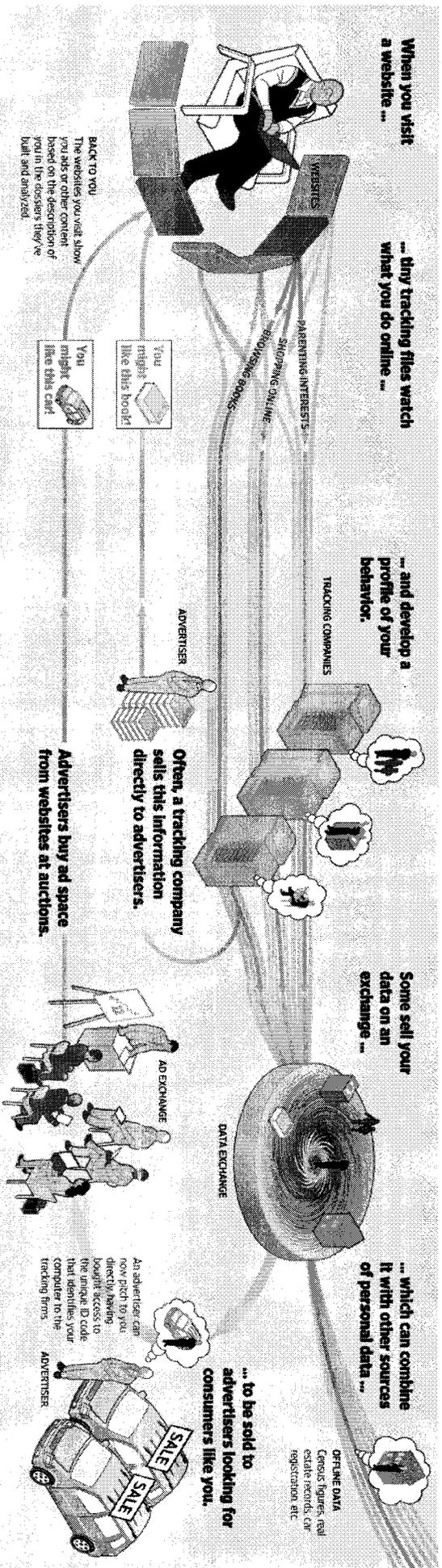


Image source: <http://graphicsweb.wsj.com/documents/divSlider/ecosystems100730.html>

A [Wall Street] Journal investigation finds that one of the fastest-growing businesses on the Internet is the business of spying on consumers. Consumer tracking is the foundation of an online advertising economy that racked up \$23 billion in ad spending last year. Tracking activity is exploding. Researchers at AT&T Labs and Worcester Polytechnic Institute last fall found tracking technology on 80% of 1,000 popular sites, up from 40% of those sites in 2005.

The Journal found tracking files that collect sensitive health and financial data. On Encyclopaedia Britannica Inc.'s dictionary website Merriam-Webster.com, one tracking file from Healthline Networks Inc., an ad network, scans the page a user is viewing and targets ads related to what it sees there. So, for example, a person looking up depression-related words could see Healthline ads for depression treatments on that page—and on subsequent pages viewed on other sites.

...Targeted ads can get personal. Last year, Julia Preston, a 32-year-old education-software designer in Austin, Texas, researched uterine disorders online. Soon after, she started noticing fertility ads on sites she visited. She now knows she doesn't have a disorder, but still gets the ads. It's "unnerving," she says.

Source: "The Web's New Gold Mine: Your Secrets" - The Wall Street Journal, 7/30/2010  
<http://online.wsj.com/article/SB100014240527487039409045753395073512989404.html>

## **Children Tracked on the Web**

A Wall Street Journal investigation into online privacy has found that **popular children's websites install more tracking technologies** on personal computers than do the top websites aimed at adults.

The Journal examined 50 sites popular with U.S. teens and children to see what tracking tools they installed on a test computer. As a group, the sites placed 4,123 "cookies," "beacons" and other pieces of tracking technology. That is 30% more than were found in an analysis of the 50 most popular U.S. sites overall, which are generally aimed at adults.

...**Selling the data is legal, but controversial**, especially when it involves young people. Two companies identified by the Journal as selling teen data initially denied doing so. Only when shown evidence that they were offering data for sale—in one case, it was labeled "teeny boppers"—did they confirm it.

Source: "On the Web, Children Face Intensive Tracking" - The Wall Street Journal, 9/17/2010

<http://online.wsj.com/article/SB10001424052748703904304575497903523187146.html>

---

## **Price Discrimination and Loan Evaluation:**

...New York-based Demdex Inc., for instance, helps websites build "behavioral data banks" that tap sources including **online-browsing records, retail purchases** and a database predicting a person's **spot in a corporate hierarchy**.

"If we've identified a visitor as a midlife-crisis male," says Demdex CEO Randy Nicolau, a client, such as an auto retailer, can "give him a different experience than a young mother with a new family." The guy sees a red convertible, the mom a minivan.

The technology **raises the prospect that different visitors to a website could see different prices as well**. Price discrimination is generally legal, so long as it's not based on race, gender or geography, which can be deemed "redlining."

In financial services, fair-lending laws prohibit discrimination based on race, color, religion, national origin, gender, receipt of public assistance or marital status. The laws also require that borrowers have access to any data used to evaluate their creditworthiness.

But the law doesn't specifically bar using web-browsing history to make lending decisions. That means, in theory, **a bank could deny a loan based on knowledge of the applicant's visits to, say, gambling sites**.

Source: "The Web's Cutting Edge, Anonymous in Name Only" - The Wall Street Journal, 8/4/2010

<http://online.wsj.com/article/SB10001424052748703294904575385532109190198.html>

---

## **Matching Real Names to Web Browsing (and more)**

...[P]ossessing real names means RapLeaf can build **extraordinarily intimate databases** on people by tapping voter-registration files, shopping histories, social-networking activities and real estate records, among other things.

"Holy smokes," says Mrs. Twombly, 67 years old, after The Wall Street Journal decoded the information in RapLeaf's file on her. **"It is like a watchdog is watching me, and it is not good."**

Source: "A Web Pioneer Profiles Users by Name," The Wall Street Journal, 10/25/2010

<http://online.wsj.com/article/SB10001424052702304410504575560243259416072.html>