

COVER STORY



By Sam Ward, USA TODAY

Online tracking takes a scary turn

You'd be shocked at what aggregators know about you

By Byron Acohido
USA TODAY

LAS VEGAS — The coolest free stuff on the Internet actually comes at a notable price: your privacy.

For more than a decade, tracking systems have been taking note of where you go and what you search for on the Web — without your permission. And today many of the personal details you voluntarily divulge on popular websites and social networks are being similarly tracked and analyzed.

The purpose for all of this online snooping is

singular: Google, Microsoft, Yahoo, Apple, Facebook and others are intent on delivering more relevant online ads to each and every one of us — and bagging that advertising money.

Trouble is, the tracking data culled from your Internet searches and surfing can get commingled with the information you disclose at websites for shopping, travel, health or jobs. And it's now possible to toss into this mix many of the personal disclosures you make on popular social networks, along with the preferences you may express via all those nifty Web applications that trigger cool services on your mobile devices.

As digital shadowing escalates, so too have concerns about the erosion of traditional notions of privacy. Privacy advocates have long fretted that health companies, insurers, lenders, employers, lawyers, regulators and law

Please see COVER STORY next page ►

USA
TODAY

Money
SECTION B

MONEY.USATODAY.COM

THURSDAY, AUGUST 4, 2011

'It is a mistake to consider (online) tracking benign'

Continued from 1B

enforcement could begin to acquire detailed profiles derived from tracking data to use unfairly against people. Indeed, new research shows that as tracking technologies advance, and as more participants join the burgeoning tracking industry, the opportunities for privacy invasion are rising.

COVER STORY

"It is a mistake to consider (online) tracking benign," cautions Sagi Leizerov, executive director of Ernst & Young's privacy services. "It's both an opportunity for amazing connections of data, as well as a time bomb of revealing personal information you assume will be kept private."

These developments are acting like kerosene on the already contentious national debates in Congress over how privacy ought to be recast to fit the Internet age. Much is at stake. The corporations involved are vying for the juiciest claims on a golden vein. Research firm eMarketer projects global spending for online ads to climb to \$132 billion by 2015, up from \$80.2 billion this year.

The technology, retail and media giants shaping this brave new world of online advertising insist that they respect — and can be trusted to preserve — individuals' privacy, even as they compete to dissect each person's likes and dislikes.

Tracking mobile apps

However, startling findings, to be released today here at the Black Hat security conference, indicate otherwise. Website security company Dasient recently found examples of PC-based tracking techniques getting extended in a troublesome way to Internet-connected mobile devices.

Dasient analyzed 10,000 free mobile apps that enable gaming, financial services, entertainment and other services on Google Android smartphones. Researchers found more than 8%, or 842, of the Android apps took the unusual step of asking users' permission to access the handset's International Mobile Equipment Identity number, the unique code assigned to each cell-phone. The IMEI was then employed as the user ID for the given app. In a number of instances, the app subsequently forwarded the user's IMEI on to an online advertising network, says

Online ad revenue

What each company will reap in 2011¹ from U.S. advertisers (in billions):

Google	\$12.8
Yahoo	\$3.5
Facebook	\$2.2
Microsoft	\$1.9
AOL	\$0.9
MySpace	\$0.2
Twitter	\$0.1

1 — projected
Source: eMarketer

By Robert W. Ahrens, USA TODAY

Neil Daswani, Dasient's chief technology officer.

"The fact that an ad network is getting your IMEI means they can know how long you've used your phone and which mobile apps you use most often," Daswani says. "The full implications of this aren't clear, but with privacy you've got to be careful."

Should IMEIs emerge as the preferred way for mobile app companies to track consumers' access to free services, the advertising industry would suddenly have a powerful new way to snoop on how you use your smartphone or tablet PC, Daswani says.

The pervasive embedding of cool location-tracking technology in mobile devices only heightens such concerns. Sen. Al Franken, D-Minn., earlier this summer introduced a bill that would restrict location tracking, partly to protect children.

Anup Ghosh, chief executive of Web browser security firm Invincea, says Dasient's findings underscore how application developers tend to grab for as much tracking data as they can without thinking through the privacy consequences.

Invincea has begun working on technology that will enable consumers to automatically disable mobile apps that

try to tap into IMEI or take other invasive actions. "The reality is, users can't be bothered to tweak privacy settings," Ghosh says.

Privacy leaks

Meanwhile, in other research, Balachander Krishnamurthy at AT&T Labs Research and Craig E. Wills of Worcester Polytechnic Institute recently discovered hard evidence of what many privacy advocates feared: Tracking data about what pages you click to are increasingly getting commingled with personal information you disclose on popular websites and on the premier social networks in alarming ways.

In one case, the researchers documented how the supplier of a Facebook music-sharing application automatically forwarded Facebook members' profile information onto a tracking data aggregator.

Facebook spokesman Brandon McCormick says the company strives to prevent such privacy leakages. Facebook requires users to grant explicit permission for any Web app company to access any Facebook profiles. And he says the company strictly forbids app companies from dispersing any Facebook profile information.

"If we find app developers commingling that data or sharing it with other parties, we will kick them off of our platform," McCormick says.

However, policing the teeming world of Web app development is a gargantuan task, says Michael Fertik, CEO of privacy services firm Reputation.com.

Tens of thousands of new Web apps get integrated into the top social networks as well as the most visited media, entertainment and shopping websites every day.

Many of the new Web app features, such as 'like' buttons and instant polls, are designed expressly to extend tracking systems and feed ever more data about users' online behaviors to the ad networks and tracking data aggregators. Data routinely get "daisy-chained" together to create individual behavioral profiles, Fertik says.

"These profiles are bought and sold to data brokers, marketers and others and are used to make decisions and judgments about you, without your knowledge, without your consent and without a way to fix inevitable errors." Fertik says. "That's what's scary."

How to limit tracking

► **Delete cookies:** SlimCleaner is a free tool that will automatically delete tracking cookies while preserving account logon cookies.

► **Erase histories:** Easy Eraser is paid software that periodically cleans sensitive information from your computer.

► **Lock down Facebook:** uProtect is a free tool that can help block your Facebook activities from being accessed by ad networks.

Source: USA TODAY research

Responding to such concerns, the Federal Trade Commission late last year called for a "Do Not Track" mechanism that would enable consumers to opt out of being tailed around the Web. The technology is simple and can be quickly added to any Web browser. Users would then be able to check a box configuring their browser to automatically notify every webpage they visit not to track them. The catch: The online advertising industry would have to universally honor Do Not Track requests.

In May, Sen. Jay Rockefeller, D-W.Va., introduced Do Not Track legislation that has gained the backing of privacy groups. Rockefeller's proposal would help consumers "decide for themselves whether or not they want to share personal information, including their various Internet and mobile Web activities," says Jeffrey Chester, executive director of the Center for Digital Democracy.

The online advertising industry prefers self-regulation. Attorney Christopher Wolf, a privacy expert at law firm Hogan Lovells, counters that a Do Not Track law "may lead to the Internet economy — one of the few economic bright spots — being shackled."

'Trust us'

As this debate intensifies, fresh findings of privacy leaks continue to turn up. Krishnamurthy and Wills recently discovered that when they used the search function on popular health websites to look up information on pancreatic cancer, nine of 10 health sites forwarded their query onto a data aggregator.

Similarly, when they filled out job applications on big-name employment sites, eight of 10 jobs sites zipped that

information over to a data aggregator, including the user's name and e-mail address. In some instances, sensitive health-related search queries and personal information gleaned from job applications were forwarded to the same aggregator.

Wills says it would have been trivial for the data aggregator to correlate the cancer query and the job application data as having certainly come from the same browser, very likely from the same person.

"It is undeniable that data aggregators are getting this sensitive personal information about me," Wills says. "We have hard evidence in our research that shows they are receiving this information. What they are doing with it, that we don't know."

Google, Microsoft, Yahoo, Adobe, AOL, Coremetrics and Quantserve are among the largest data aggregators. They each operate sprawling networks of tracking systems that encompass dozens more smaller, independent ad networks, data analytics firms and tracking services.

Google, reportedly the largest data aggregator, has long taken the public position that its tracking systems use an alphanumeric code to identify and keep track of individual Web browsers, and that it simply does not correlate any personal information to these anonymous browser identifiers.

After reviewing copies of Krishnamurthy and Wills' research, Google spokesman Rob Shilkin issued a statement: "We've never attempted or wanted to use any personal or sensitive information in any URLs provided by a third party, and in fact this very issue is addressed by the comprehensive self-regulatory schemes that we comply with."

Google has been widely known to scan the contents of Gmail messages to deliver targeted text ads. While some don't mind, others believe scanning e-mail to deliver more relevant ads is an invasion of privacy. John Simpson, spokesman for the non-profit advocacy group Consumer Watchdog, isn't convinced the search giant will necessarily stop there.

"Part of the problem is that Google collects and stores tremendous amounts of data about its users," Simpson says. "The only assurance we have about what Google's intentions are boils down to 'Trust us.'"