A Journal investigation finds that one of the fastest-growing businesses on the Internet is the business of spying on consumers. First in a series. By Julia Angwin

THE WEB'S NEW GOLD MINE: YOUR SECRETS

Hidden inside Ashley Hayes-Beaty's computer, a tiny file helps gather personal details about her, all to be put up for sale for a tenth of a penny. The file consists of a single code—4c8126b292a72b95e5416a323e79bd37—that secretly identifies her as a 26-year-old female in Nashville, Tenn. The code knows that her favorite movies include "The Princess Bride," "50 First Dates," and "10 Things I Hate About You." It knows she enjoys the "Sex and the City" series. It knows she browses entertainment news and likes to take quizzes.

"Well, I like to think I have some mystery left to me, but apparently not!" Ms. Hayes-Beaty said when told what that snippet of code reveals about her.

"The profile is eerily correct." Ms. Hayes-Beaty is being monitored by Lotame Solutions Inc., a New York company that uses sophisticated software called "beacon" to capture what people are typing on a website—their comments on movies, say, or their interest in parenting and pregnancy. Lotame packages that data into profiles about individuals, without determining a person's name, and sells the profiles to companies seeking customers. Ms. Hayes-Beaty's tastes can be sold wholesale (a batch of movie lovers is $1 per thousand) or customized (25-year-old Southern fans of "50 First Dates").

"We can segment it all the way down to one person," says Eric Perros, Lotame's chief marketing officer. One of the fastest-growing businesses on the Internet, a Wall Street Journal investigation has found, is the business of spying on Internet users.

The Journal conducted a comprehensive study that assesses and analyzes the broad array of cookies and
other surveillance technology that companies are deploying on Internet users. It reveals that the tracking of consumers has grown both far more pervasive and far more intrusive than is realized by all but a handful of people in the vanguard of the industry.

The study found that the nation's 50 top Web sites average installed 64 pieces of tracking technology onto the computers of visitors, usually with no warning. A dozen sites each installed more than a hundred. The nonprofit Workshop installed none.

- Tracking technology is getting smarter and more intrusive. Monitoring used to mean checking files on a user's computer for cookies — files that record websites people visit.

- The new technologies are transforming the Internet economy. Advertisers once primarily bought ads on specific Web pages on a car ad on a car site. Now, advertisers are willing to pay a premium to follow people around the Internet, wherever they go, with highly specific marketing messages.

- In between the Internet user and the advertiser, the Journal identified more than 100 middlemen-tracking companies, data brokers and advertising networks — competing to meet the growing demand for data on individual behavior and interests.

- The data on Ms. Hayes-Beatty's filming habits, for instance, is being offered to advertisers on a single-source basis, one of the new data exchanges.

- It is a sea change in the way the industry works," says Omar Tawafou, CEO of Bluekai. "Advertisers want to buy access to people, not Web pages."

- The Journal examined the 50 most popular U.S. websites, which account for about 40% of the time people spend on the web. Of those websites, 87% are currently used by Americans. The Journal also tested its own site. In July, the Journal then analyzed the tracking files and programs these sites downloaded onto the Journal's test computer.

- As a group, the top 50 sites placed 3,180 tracking files in total on the Journal's test computer. Nearly a third of these were invisible, deployed to remember past visitors on a favorite site or simply to monitor page visits.

- But over two-thirds — 2,224 — were installed by 131 companies, many of which are in the business of tracking Web users to create rich databases of consumer profiles that can be sold.

- The top venue for such technology, the Journal found, was the interactive Corp's Dictionary.com. A visit to the online dictionary site resulted in 134 files or programs being downloaded onto the Journal's test computer, 223 of which were known to be tracking Web users.

- The information that companies gather is anonymous, in the sense that Internet users are identified by a number assigned to their computer, not by a specific person's name. Lotame, for instance, says it doesn't know the name of users such as Ms. Hayes-Beatty — only their behavior and attributes, identified by a random number. People who don't want to be tracked can remove themselves from Lotame's system.

- And the industry says the data are used appropriately. David Moss, chairman of 737 RealMedia Inc., an ad network owned by WPP PLC, says tracking gives Internet users better advertising.

- "When an ad is targeted properly, it's more effective, it's more relevant. It's more important information," he says.

- Tracking isn't new. But the technology is growing so powerful and ubiquitous that even some of America's biggest sites say they were unaware, until informed by the Journal, that they were installing intrusive files on visitors' computers.

- The Journal found that Microsoft Corp.'s popular Windows update, MSN.com, placed a tracking file onto their computer.

- "When an ad is targeted properly, it's more effective, it's more relevant. It's more important information," he says.

- Tracking isn't new. But the technology is growing so powerful and ubiquitous that even some of America's biggest sites say they were unaware, until informed by the Journal, that they were installing intrusive files on visitors' computers.

- The Journal found that Microsoft Corp.'s popular Windows update, MSN.com, placed a tracking file onto their computer.

- "When an ad is targeted properly, it's more effective, it's more relevant. It's more important information," he says.

- Tracking isn't new. But the technology is growing so powerful and ubiquitous that even some of America's biggest sites say they were unaware, until informed by the Journal, that they were installing intrusive files on visitors' computers.

- The Journal found that Microsoft Corp.'s popular Windows update, MSN.com, placed a tracking file onto their computer.
Glossary

Data exchange
A marketplace where advertisers bid for access to data about customers. Marketers then use this data to target ads. For example, a Denver hotel might bid to reach people known to have researched Denver hotels recently.

Offline data
Information that you collect from sources other than the Internet. It could include your zip code, estimated household income, the cars you own or the purchases you’ve made in a store.

Privacy policy
A notice on a website that discloses how the site collects or uses information.

Third-party tracking tool
A cookie, beacon or other tracking technology installed on your computer by an ad network or research firm that can track your activities across many websites.

Tracking company
Companies that use cookies and other tracking technology to collect online data about you.

Ad network
A company that sells ads on behalf of website publishers.

Aggregated information
Data combined from many individual users that can’t identify anyone personally.

Invisible software on many websites (also known as “bugs” or “pixels”) that can track web surfers’ locations and activities online. Some are powerful enough to know what a user types on a particular site.

Exposure index
The Journal’s analysis to determine how much each site exposes visitors to intrusive monitoring. Each tracker was given a score based on how the tracking company collects, shares, and uses your data. A website’s exposure index was calculated using the sum of the scores of the trackers we found on that site.

Flash cookie
Small file put on your computer by Adobe’s Flash software, which is used by many sites to display video ads. Flash cookies can be designed to reinstall regular cookies that were previously deleted.

User profile
Information about your actions, interests and characteristics that tracking companies compile about you.

More from the project at WSJ.com/WTX

What exactly is a cookie?
Watch a short video guide to learn how advertisers use them to track your online habits.

Get step-by-step instructions on how to delete cookies and use your browser’s privacy options to protect against being tracked.

Cookie
Tiny text file put on your PC by websites or marketing firms that—depending on its purpose—might be used simply to remember your preferences for one site, or to track you across many sites.

First-party tracking tool
Typically, a cookie installed on your computer by a website for benign purposes such as keeping you logged in to that one site.

Getting the dot-com boom of the late 1990s, advertisers were buying ads based on proximity to content—shoe ads on fashion sites.

The dot-com bust triggered a power shift in online advertising, away from websites and toward advertisers. Advertisers began paying for ads only if someone clicked on them. Sites and ad networks began using cookies aggressively in hopes of showing ads to people most likely to click on them, thus getting paid.

Targeted ads command a premium. Last year, the average cost of a targeted ad was $4.12 per thousand viewers, compared with $1.98 per thousand viewers for an untargeted ad, according to an ad-industry-sponsored study in March.

The Journal examines three kinds of tracking technology—basic cookies as well as more powerful “Flash” cookies and bits of software code called “beacons.”

More than half of the sites examined by the Journal installed 23 or more “third-party” cookies. Dictionary.com installed the most, placing 159 third-party cookies.

Cookies are typically used by tracking companies to build lists of pages visited from a specific computer. A newer type of technology, beacons, can watch even more activity.

Beacons, also known as “Web bugs” and “pixels,” are small pieces of software that run on a Web page. They can track what a user is doing on the page, including what is being typed or where the mouse is moving.

The majority of sites examined by the Journal placed at least seven beacons from outside companies. Dictionary.com had the most, 41, including several from companies that track health conditions and one that says it can target consumers by dozens of factors, including zip code and race.

Dictionary.com President Shravan Goli attributed the presence of so many tracking tools to the fact that the site was working with a large network of ad networks, each of which places its own cookies and beacons. After the Journal contacted the company, it cut the number of networks it uses and beefed up its privacy policy to more fully disclose its practices.

The widespread use of Adobe Systems Inc.’s Flash software to play videos online offers another opportunity to track people. Flash cookies originally were meant to remember users’ preferences, such as volume settings for online videos.

But Flash cookies can also be
used by data collectors to re-in-
stall regular cookies that a user
has deleted. This can circumvent
a user's attempt to avoid being
tracked online. Adobe condemns
the practice.

Most sites examined by the
Journal installed no Flash cook-
ies. Comcast.net installed 55.

That finding surprised the
company, which said it was un-
aware of them. Comcast Corp.
subsequently determined that it
had used a piece of free software
from a company called Clear-
spring Technologies Inc. to
display a slideshow of celebrity
photos on Comcast.net. The
Flash cookies were installed on
Comcast's site by that slideshow,
according to Comcast.

Clearspring, based in
McLean, Va., says the 55 Flash
cookies were a mistake. The
company says it no longer uses
Flash cookies for tracking.

CEO Hooman Radfar says
Clearspring provides software
and services to websites at no
charge. In exchange, Clearspring
collects data on consumers. It
plans eventually to sell the data
it collects to advertisers, he
says, so that site users can be
shown "ads that don't suck." 
Comcast's data won't be used,
Clearspring says.

Wittingly or not, people pay
a price in reduced privacy for
the information and services
they receive online. Diction-
ary.com, the site with the most
tracking files, is a case study.

The site's annual revenue,
about $9 million in 2009 accordin-
g to an SEC filing, means the
site is too small to support an
extensive ad-sales team. So it
needs to rely on the national
ad-placing networks, whose busi-
ness model is built on tracking.

Dictionary.com executives say
the trade-off is fair for their
users, who get free access to its
dictionary and thesaurus service.

"Whether it's one or 10 cook-
ies, it doesn't have any impact
on the customer experience, and
we disclose we do it," says Dic-
tionary.com spokesman Nicholas
Graham. "So what's the beef?"

The problem, say some in-
dustry veterans, is that so much
consumer data is now up for
sale, and there are no legal lim-
its on how that data can be used.

Until recently, targeting con-
sumers by health or financial
status was considered off-limits
by many large Internet ad com-
panies. Now, some aim to take
targeting to a new level by tap-

When you visit
a website ...

... tiny tracking files watch
what you do online ...

BACK TO YOU
The websites you visit show
you ads or other content
based on the description of
you in the dossiers they've
built and analyzed.

Ashley Hayes-Beaty's taste in film is tracked by a New York firm—and offered for sale for a tenth of a cent.
ping online social networks.

Media6Degrees Inc., whose technology was found on three sites by the Journal, is pitching banks to use its data to size up consumers based on their social connections. The idea is that the creditworthy tend to hang out with the creditworthy, and deadbeats with deadbeats.

"There are applications of this technology that can be very powerful," says Tom Phillips, CEO of Media6Degrees. "Who knows how far we'd take it."

—Emily Steel, Jennifer Valentino-DeVries and Tom McGinty contributed to this report.
Microsoft Quashed Effort To Boost Online Privacy

BY NICK WINGFIELD

The online habits of most people who use the world’s dominant Web browser are an open book to advertisers. That wasn’t the plan at first.

In early 2008, Microsoft Corp.’s product planners for the Internet Explorer 8.0 browser intended to give users a simple, effective way to avoid being tracked online. They wanted to design the software to automatically thwart common tracking tools, unless a user deliberately switched to settings affording less privacy.

That triggered heated debate inside Microsoft. As the leading maker of Web browsers, the gateway software to the Internet, Microsoft must balance conflicting interests: helping people surf the Web with its browser to keep their mouse clicks private, and helping advertisers who want to see those clicks.

In the end, the product planners lost a key part of the debate. The winners: executives who argued that giving automatic privacy to consumers would make it tougher for Microsoft to profit from selling online ads. Microsoft built its browser so that users must deliberately turn on privacy settings every time they start up the software.

Microsoft’s original privacy plans for the new Explorer were “industry-leading” and technically superior to privacy features in earlier browsers, says Simon Davies, a privacy-rights advocate in the U.K. whom Microsoft consulted while forming its browser privacy plans. Most users of the final product aren’t even aware its privacy settings are available, he says. “That’s where the disappointment lies.”

Microsoft General Counsel Brad Smith says that in developing the new browsers, the company tried to “synthesize” both points of view about privacy “in a way that advanced both the privacy interests of consumers and the critical role advertising plays in content.”

Microsoft’s decision reveals the economic forces driving the spread of online tracking of individuals. A Wall Street Journal investigation of the practice showed tracking to be pervasive and ever-more intrusive: The 50 most-popular U.S. websites, including four run by Microsoft, installed an average of 64 pieces of tracking technology each on a test computer.

As online advertising grows more sophisticated, companies playing prominent roles in consumers’ online experiences have discovered they have access to a valuable trove of information.

In addition to Microsoft, such companies include search-engine giant Google Inc., iPhone maker Apple Inc., and Adobe Systems Inc., whose Flash software makes much of the Internet’s video, gaming and animation possible. These companies now have a big say in how much information can be collected about individual users.

Many also have big stakes in online advertising. Microsoft bought aQuantive, a Web-ad firm, in 2007 for more than $6 billion, to build a business selling ads online. Google, already a giant in online marketing, in September 2008 launched a Web browser, Chrome, that gives it new insight into Internet users’ habits. Apple has launched an ad network, iAds, for its iPhone and iPad. And Adobe last year paid $1.5 billion to buy Omniture, which measures the effectiveness of online ads.

Executives in Microsoft’s new ad business were upset when the designers of Internet Explorer hatched the plan to block tracking activity, say people involved in the debate. At a meeting in the spring of 2008, Brian McAndrews, a Microsoft senior vice president who had been chief executive of aQuantive before Microsoft acquired it, complained to the browser planners. Their privacy plan, he argued, would disrupt the selling of Web ads by Microsoft and other companies, these people say.

Mr. McAndrews was taken aback that Explorer planners seemed unwilling to accept input from advertising executives, given that Microsoft had spent $6 billion on a Web-ad firm, according two people who participated in the meeting.

Mr. Smith, the general counsel, says Microsoft weighed both sides of the argument in its debate. He says the company was concerned about the effect strict privacy features might have on free sites supported by advertising, including newspaper sites.

Such sites, including WSJ.com, use information derived from tracking to sell targeted ads, an important revenue source.

Web browsers like Internet Explorer can play an important role in protecting privacy because the software sits between consumers and the array of technologies used to track them online. The best-known of those technologies are browser “cookies,” small files stored on users’

![Browser Battle](Image)

Competitors have chipped away at Microsoft’s market share.

<table>
<thead>
<tr>
<th>2008</th>
<th>2009</th>
<th>2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>80%</td>
<td>80%</td>
<td>80%</td>
</tr>
<tr>
<td>60%</td>
<td>60%</td>
<td>60%</td>
</tr>
<tr>
<td>40%</td>
<td>40%</td>
<td>40%</td>
</tr>
<tr>
<td>20%</td>
<td>20%</td>
<td>20%</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Source: NetApplications.com

computers that act as identification tags for them when they visit websites.

Some cookies, such as those installed when a user asks a favorite website to remember his password, don’t do tracking.

Others are installed on computers by companies that provide advertising services to the
websites a user visits. These “third-party” cookies can be designed to track a user’s online activities over time, building a database of personal interests and other details.

The Journal’s examination of the top 50 most popular U.S. websites showed that Microsoft placed third-party tracking devices on 27 of the top 46 sites that it doesn’t own itself.

All the latest Web browsers, including Internet Explorer, let consumers turn on a feature that prevents third-party browser cookies from being installed on their computers. But those settings aren’t always easy to find. Only one major browser, Apple’s Safari, is preset to block all third-party cookies, in the interest of user privacy.

“Only browser developers have the resources and large user bases necessary to create a privacy-friendly version of the Web,” says Peter Eckersley, staff technologist with the Electronic Frontier Foundation, a digital-rights advocacy group.

Because Internet Explorer is used by so many people—nearly 60% of all Web users—the 2008 decision by planners of the new version to make it easy for users to block tracking could have had a big effect on the marketplace.

At the time, the practice of tailoring ads to consumers based on their browsing habits was taking off. Google was in the process of buying DoubleClick Inc., a leader in the placing and tracking of online ads, for $3.1 billion.

A coalition of privacy groups was petitioning the Federal Trade Commission to develop stricter policies for preventing advertisers from tracking Web-browsing habits. Companies with stakes in Internet advertising were feeling heat to try to stave off government regulation by voluntarily protecting consumer privacy.

Microsoft also was trying to stem the erosion of its browser market share. Internet Explorer, which once had more than 95% of the market, hadn’t kept up with competitors. Firefox, a Web browser overseen by the nonprofit Mozilla Foundation, picked up more than 18% of the market by May 2008, helping knock Explorer to 76%, according to NetApplications.com, which tracks browser use.

The browser planners at Microsoft believed aggressive new privacy features could help differentiate the new Internet Explorer from rivals, according to several current and former Microsoft executives.

The planners, led by Microsoft veteran Dean Hachamovitch, came up with a concept for preventing consumer tracking. A new feature would monitor where each piece of content on a visited Web page was originating on the Internet—every picture, video or chunk of text.

The feature would pay special attention to content from “third-party” Internet addresses—addresses different from the one a user sees in the address bar at the top of the browser.

Some of that third-party content could be innocuous things like YouTube video clips displayed on the Web page, which viewers probably wouldn’t want to block.

Other items might be tracking tools such as Web “beacons,” snippets of code embedded in the page that can monitor the clicks of visitors, or even record their keystrokes. Users might want such tracking tools blocked automatically.

The Internet Explorer planners proposed a feature that would block any third-party content that turned up on more than 10 visited websites, figuring that anything so pervasive was likely to be a tracking tool. This, they believed, was a more comprehensive approach to privacy than simply turning off browser cookies, one that would thwart other tracking methods.

The group also planned to design the Internet Explorer setup process so that it guaranteed the privacy feature would be used by most people.

When he heard of the ideas, Mr. McAndrews, the executive involved with Microsoft’s Internet advertising business, was angry, according to several people familiar with the matter. Mr. McAndrews feared the Explorer group’s privacy plans would dramatically reduce the effectiveness of online advertising by curbing the data that could be collected about consumers.

He heard about the proposal through back channels rather than directly from the browser planners, these people say, which surprised him given its implications. Some people who worked in the browser group acknowledged that they should have been more upfront about their intentions. Mr. McAndrews later left the company.

“We were worried it was going to cause a stampede” away from tracking technologies, says an executive who worked with Mr. McAndrews. “It was an act with the potential to reverberate across the industry.”

The browser group and its manager, Mr. Hachamovitch, tried to hold their ground. They were reluctant to let advertising executives interfere with the new Explorer design, according to people involved in the debate. Microsoft said that Mr. Hachamovitch and other members of the planning group wouldn’t comment on the matter.

The debate widened after executives from Microsoft’s advertising team informed outside advertising and online-publishing groups of Microsoft’s privacy plans for Explorer. Microsoft Chief Executive Steve Ballmer assigned two senior executives, chief research and strategy officer Craig Mundie and the general counsel, Mr. Smith, to help referee the debate, according to Peter Cullen, Microsoft’s chief privacy strategist.

The two men convened a four-hour meeting in Mr. Mundie’s conference room in late spring 2008 to allow outside organizations to voice their concerns, including the Interactive Advertising Bureau, the Online Publishers’ Association and the American Association of Advertising Agencies.

One of the attendees, Interactive Advertising Bureau Chief Executive Randall Rothenberg, says he was worried that Explorer’s proposed privacy features would block not just the collection of consumer data, but also the delivery of some Web advertisements themselves. He says the features “seemed to equate the delivery of advertisements with privacy violations.”

He was especially troubled, he says, by the prospect of Microsoft turning the features on for all consumers, by default.

One other consideration: Some Microsoft executives were concerned that the preset-privacy plan might jeopardize support among ad-industry organizations that Microsoft wanted to rally against a proposed advertising deal between Google and Yahoo Inc., a Microsoft executive. A Microsoft spokeswoman declined to comment on that issue. U.S. regulators ended up blocking the deal.

The former Microsoft executive says he had never before experienced a debate at Microsoft “so driven by external influences and conflicting priorities to protect users” as the tussle over the Explorer privacy controls.

“It was a healthy debate,” says Mr. Smith, the general counsel, with “well-informed views by people who are passionate.”

When Microsoft released the browser in its final form in March 2009, the privacy features were a lot different from what its planners had envisioned. Internet Explorer required the consumer to turn on the feature that blocks tracking by websites, called InPrivate Filtering. It wasn’t activated automatically.

What’s more, even if consumers turn the feature on, Microsoft designed the browser so InPrivate Filtering doesn’t stay on permanently. Users must activate the privacy setting every time they start up the browser.

Microsoft dropped another proposed feature, known as InPrivate Subscriptions, that would have let users further conceal their online browsing habits, by automatically blocking Web addresses suspected of consumer tracking if those addresses appeared on “black lists” compiled by privacy groups.

Mr. Cullen, Microsoft’s chief privacy strategist, says the input of outsiders helped Microsoft strike a balance between privacy and advertising interests. The browser, he says, “was a better product than when it came off the drawing-room floor of the Internet Explorer group.”

Advertising groups say they were pleased, too. “They ended up with something pretty excellent,” says Mr. Rothenberg of the Interactive Advertising Bureau.
A business that is focused on tracking people online...  

- 99% have Flash installed on all Internet-enabled PCs  
- 26% of U.S. Internet searches  
- 63% of U.S. Internet  
- 60% browser market share of global

Microsoft and other companies whose products define the way people use the Internet...
Clockwise from top left: Former Microsoft executive Brian McAndrews, who complained about a proposed privacy plan; Microsoft General Counsel Brad Smith and chief research and strategy officer Craig Mundie refereed the debate. Interactive Advertising Bureau CEO Randall Rothenberg.

**Coming Next**
Cutting-edge websites delve into your finances—before you divulge a single fact.

**WSJ.com/WTK**
What They Know

Explore an online database of the tracking practices of the top 50 U.S. websites.

**Data analysis**
Tom McGinty, Scott Thurm, Julia Angwin, Courtney Banks and Marisa Taylor

**How to remove tracking files from Internet Explorer**
In the toolbar at the top, click Tools, then select Internet Options. This will bring up a new window. Here, the button to easily delete all cookies is next to Settings under Browsing History. To delete only certain cookies, click Settings instead of Delete.

You can also adjust your browser settings to block and accept some cookies ...

... and use InPrivate Browsing and InPrivate Filtering if you have IE8.

**GET STEP-BY-STEP INSTRUCTIONS ON HOW TO DELETE COOKIES FROM OTHER BROWSERS: WSJ.com/WTK**
Your Apps Are Watching You

A Journal investigation finds that iPhone and Android apps are breaching the privacy of smartphone users.

BY SCOTT THURM AND YUKARI IWATANI KANE

FEW DEVICES KNOW more personal details about people than the smartphones in their pockets: phone numbers, current location, often the owner’s real name—even a unique ID number that can never be changed or turned off.

These phones don’t keep secrets. They are sharing this personal data widely and regularly, a Wall Street Journal investigation has found.

An examination of 101 popular smartphone “apps”—games and other software applications for iPhone and Android phones—showed that 56 transmitted the phone’s unique device ID to other companies without users’ awareness or consent. Forty-seven apps transmitted the phone’s location in some way. Five sent age, gender and other personal details to outsiders.

The findings reveal the intrusive effort by online-tracking companies to gather personal data about people in order to flesh out detailed dossiers on them.

Among the apps tested, the iPhone apps transmitted more data than the apps on phones using Google Inc.’s Android operating system. Because of the test’s size, it’s not known if the pattern holds among the hundreds of thou-
WHAT THEY KNOW

A WALL STREET JOURNAL INVESTIGATION

Apple says iPhone apps “cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used.” Many apps tested by the Journal appeared to violate that rule, by sending a user’s location to ad networks, without informing users. Apple declines to discuss how it interprets or enforces the policy.

Phones running Google’s Android operating system are made by companies including Motorola Inc. and Samsung Electronics Co. Google doesn’t review the apps, which can be downloaded from many vendors. Google says app makers “bear the responsibility for how they handle user information.”

Google requires Android apps to notify users, before they download the app, of the data sources the app intends to access. Possible sources include the phone’s camera, memory, contact list, and more than 100 others. If users don’t like what a particular app wants to access, they can choose not to install the app, Google says.

“Our focus is making sure that users have control over what apps they install, and notice of what information the app accesses,” a Google spokesman says.

Neither Apple nor Google requires apps to ask permission to access some forms of the device ID, or to send it to outsiders. When smartphone users let an app see their location, apps generally don’t disclose if they will pass the location to ad companies.

Lack of standard practices means different companies treat the same information differently. For example, Apple says that, internally, it treats the iPhone’s UDID as “personally identifiable information.” That’s because, Apple says, it can be combined with other personal details about people—such as names or email addresses—that Apple has via the App Store or its iTunes music services. By contrast, Google and most app makers don’t consider device IDs to be identifying information.

A growing industry is assembling this data into profiles of cellphone users. Mobicip, the ad exchange, matches more than 25 ad networks with some 15,000 apps seeking advertisers. The Palo Alto, Calif., company collects phone IDs, encodes them (to obscure the number), and assigns them to interest categories based on what apps people download and how much time they spend using an app, among other factors.

By tracking a phone’s location, Mobi...
The personal data that your smartphone stores ...

... can be collected by the apps that you download ...

... and is often sent to outside companies.

In the Journal's tests, the music app Pandora shared personal information as shown above.

EXPLOR ALL THE APPS: WSJ.com/WTK

SERIES GRAPHICS BY ANDREW GARCIA PHILLIPS AND SARAH SLOBIN

clix also makes a "best guess" of where a person lives, says Mr. Gurbuxani, the Mobelix executive. Mobelix then matches that location with spending and demographic data from Nielsen Co.

In roughly a quarter-second, Mobelix can place a user in one of 150 "segments" it offers to advertisers, from "green enthusiasts" to "soccer moms." For example, "die hard gamers" are 16- to-23-year-olds with more than 20 apps on their phones who use an app for more than 20 minutes at a time.

Mobelix says its system is powerful, but that its categories are broad enough to not identify individuals. "It's about how you track people better," Mr. Gurbuxani says.

Some app makers have made changes in response to the findings. At least four app makers posted privacy policies after being contacted by the Journal, including Rovio Mobile Ltd., the Finnish company behind the popular game Angry Birds (in which birds battle egg-snatching pigs). A spokesman says Rovio had been working on the policy, and the Journal inquiry made it a good time to unveil it.

Free and paid versions of Angry Birds were tested on an iPhone. The apps sent the phone's UDID and location to the Chillingo unit of Electronic Arts Inc., which markets the games. Chillingo says it doesn't use the information for advertising and doesn't share it with outsiders.

Apps have been around for years, but burst into prominence when Apple opened its App Store in July 2008. Today, the App Store boasts more than 300,000 programs.

Other phone makers, including BlackBerry maker Research in Motion Ltd. and Nokia Corp., quickly built their own app stores. Google's Android Market, which opened later in 2008, has more than 100,000 apps. Market researcher Gartner Inc. estimates that world-wide app sales this year will total $6.7 billion.

Many developers offer apps for free, hoping to profit by selling ads inside the app. Noah Elkin of market researcher eMarketer says some people are "willing to tolerate advertising in apps to get something for free." Of the 101 apps tested, the paid apps generally sent less data to outsiders.

Ad sales on phones account for less than 5% of the $23 billion in annual Internet advertising. But spending on mobile ads is growing faster than the market overall.

Central to this growth: the ad networks whose business is connecting advertisers with apps. Many ad networks offer software "kits" that automatically insert ads into an app. The kits also track where users spend time inside the app.

Some developers feel pressure to release more data about people. Mike Binshtok, creator of the DailyHoroscope Android app, says ad-network executives encouraged him to transmit users' locations.

Mr. Binshtok says he declined because of privacy concerns. But ads targeted by location bring in two to five times as much money as untargeted ads, Mr. Binshtok says. "We are losing a lot of revenue."

Other apps transmitted more data. The Android app for social-network site MySpace sent age and gender, along with a device ID, to Millennial Media, a big ad network.
In its software-kit instructions, Millennial Media lists 11 types of information about people that developers may transmit to "help Millennial provide more relevant ads." They include age, gender, income, ethnicity, sexual orientation and political views. In a re-test with a more complete profile, MySpace also sent a user's income, ethnicity and parental status.

A spokesman says MySpace discloses in its privacy policy that it will share details from user profiles to help advertisers provide "more relevant ads." MySpace is a unit of News Corp., which publishes the Journal. Millennial did not respond to requests for comment on its software kit.

App makers transmitting data say it is anonymous to the outside firms that receive it. "There is no real-life I.D. here," says Joel Simkhai, CEO of Nearby Buddy Finder LLC, the maker of the Grindr app for gay men. "Because we are not tying [the information] to a name, I don't see an area of concern."

Scott Lahman, CEO of TextPlus 4 developer Gogii Inc., says his company "is dedicated to the privacy of our users. We do not share personally identifiable information or message content." A Pandora spokeswoman says, "We use listener data in accordance with our privacy policy," which discusses the app's data use, to deliver relevant advertising. When a user registers for the first time, the app asks for email address, gender, birth year and ZIP code.

Google was the biggest data recipient in the tests. Its AdMob, AdSense, Analytics and DoubleClick units collectively heard from 38 of the 101 apps. Google, whose ad units operate on both iPhones and Android phones, says it doesn't mix data received by these units.

Google's main mobile-ad network is AdMob, which it bought this year for $750 million. AdMob lets advertisers target phone users by location, type of device and "demographic data," including gender or age group.

A Google spokesman says AdMob targets ads based on what it knows about the types of people who use an app, phone location, and profile information a user has submitted to the app. "No profile of the user, their device, where they've been or what apps they've downloaded, is created or stored," he says.

Apple operates its iAd network only on the iPhone. Eighteen of the 51 iPhone apps sent information to Apple.

Apple targets ads to phone users based largely on what it knows about them through its App Store and iTunes music service. The targeting criteria can include the types of songs, videos and apps a person downloads, according to an Apple ad presentation reviewed by the Journal. The presentation named 103 targeting categories, including: karaoke, Christian/gospel music, anime, business news, health apps, games and horror movies.

People familiar with iAd say Apple doesn't track what users do inside apps and offers advertisers broad categories of people, not specific individuals.

Apple has signaled that it has ideas for targeting people more closely. In a patent application filed this past May, Apple outlined a system for placing and pricing ads based on a person's "web history or search history" and "the contents of a media library." For example, home-improvement advertisers might pay more to reach a person who downloaded do-it-yourself TV shows, the document says.

The patent application also lists another possible way to target people with ads: the contents of a friend's media library.

How would Apple learn who a cell-phone user's friends are, and what kinds of media they prefer? The patent says Apple could tap "known connections on one or more social-networking websites" or "publicly available information or private databases describing purchasing decisions, brand preferences," and other data. In September, Apple introduced a social-networking service within iTunes, called Ping, that lets users share music preferences with friends. Apple declined to comment.

Tech companies file patents on blue-sky concepts all the time, and it isn't clear whether Apple will follow through on these ideas. If it did, it would be an evolution for Chief Executive Steve Jobs, who has spoken out against intrusive tracking. At a tech conference in June, he complained about apps "that want to take a lot of your personal data and suck it up."

—Tom McGinty and Jennifer Valentino-DeVries contributed to this report.

What Can You Do?
Not Much

IT'S NEARLY IMPOSSIBLE to prevent cellphone "apps"—games and other software—from transmitting information about a phone and its owner.

Turning off the phone's location services can restrict tracking by location. But it can limit some phone features like maps.

A few mobile marketing companies offer an "opt out" that prevents the use of tracking data to deliver targeted ads on websites viewed on cellphones. But most don't apply to apps. For instance, Ringleader Digital Inc.'s opt-out at ringleaderdigital.com/optout.php applies only to Internet browsing.

Ad company Jumptap Inc. says that its opt-out (opt.jumptap.com/optout/opt?jt) also doesn't apply to apps.

However, Jumptap says iPhone users can opt out of targeted ads in apps by emailing their Unique Device Identifier, or UDID, to optout@jumptap.com. The UDID is found by connecting the phone to iTunes and clicking on the serial number shown.

Apple Inc. says the opt-out for its mobile-ad system, iAd, does work for apps because it is tied to users' iTunes accounts rather than the Web browser. The opt-out (oo.apple.com) doesn't prevent iTunes data from being collected.

Google Inc. says it doesn't offer an opt-out for ads in apps because it doesn't create profiles of app users. It says its in-app ads aren't targeted based on user profiles.

DATA ANALYSIS:
Scott Thurm
Tom McGinty
Julia Angwin
Courtney Banks
Jennifer Valentino-DeVries
# Personal Details, Exposed by Smartphone Apps

**THE JOURNAL** examined 101 popular iPhone and Android smartphone “apps” to see what personal details they transmit about their users. Data companies use information like this to track people and target ads. Here is a partial list of the findings. For an interactive database of the full results, go to WSJ.com/WTK.

<table>
<thead>
<tr>
<th>Android Apps</th>
<th>AGE</th>
<th>GENDER</th>
<th>LOCATION</th>
<th>PHONE</th>
<th>L.D.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Task Killer</td>
<td>No data flow detected</td>
<td>App collects data</td>
<td>App sends data to other companies</td>
<td>Icons display which types of data each app collected and shared with outside companies.</td>
<td></td>
</tr>
<tr>
<td>Advanced Task Killer Pro</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alchemy (Andrey Zaikin)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backgrounds (Stylem Media)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Barcode Scanner (Zxing Team)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Beautiful Widgets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bible App (LifeChurch.tv)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calorie Counter (FatSecret)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CardioTrainer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CBS News</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DailyHoroscope (Comitic)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dictionary.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ESPN ScoreCenter</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facebook</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fishin’ 2 Go</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Foursquare</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fox News</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fruit Ninja</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google Maps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Groupon</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Handcent SMS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jewels</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Labyrinth</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Labyrinth Lite</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LauncherPro</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Movies by Flixter</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MyBackup Pro</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MySpace Mobile</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NYTimes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pandora</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Paper Toss</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ringdroid</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Robo Defense</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Robo Defense Free</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shazam</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ShopSavvy Barcode Scanner</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Solitaire (Ken Magic)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Talking Tom Cat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Talking Tom Cat Free</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Coupons App</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Toss It</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TweetCaster</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>US Yellow Pages Search</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weather &amp; Toggle Widget</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Weather Channel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WeatherBug</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WeatherBug Elite</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yelp</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>YouTube</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zedge Ringtones &amp; Wallpapers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Groupon, an app for discounts from local merchants, sent phone identifiers and location information to outsiders.

The Paper Toss game sent a unique phone identifier to five ad companies and location information to three of those companies.
Personal Details, Exposed by Smartphone Apps

Icons display which types of data each app collected and shared with outside companies.

**iPhone Apps**

<table>
<thead>
<tr>
<th>App Name</th>
<th>Age</th>
<th>Gender</th>
<th>Location</th>
<th>Phone ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.03 Seconds</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>0.03 Seconds Pro</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Age My Face</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Angry Birds</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Angry Birds Lite</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Aurora Feint II: Lite</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Barcode Scanner (BahnTech)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Bejeweled 2</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Best Alarm Clock Free</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Bible App (LifeChurch.tv)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Bejeweled 2</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>CBS News</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Dictionary.com</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Doodle Jump</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>ESPN ScoreCenter</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Facebook</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Flashlight (John Haney Software)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Fluent News Reader</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Foursquare</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Fox News</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Google Maps</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Grindr</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Groupon</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Hipstamatic</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Jwheels</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>iLoveBeer: Zythology</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Medscape</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>MyFitnessPal</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Netflix</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>NYTimes</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Ninjamp</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Pandora</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Paper-Toss</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>PerfectPhoto</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Pimple Popper Lite</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Pumpkin Maker</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>RediLaser</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Ringtone Maker</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Ringtone Maker Pro</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Shazam</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Talking Tom Cat</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

**Grindr**, an app for meeting gay men, sent a user's gender, location and phone ID to three companies.

**TextPlus 4**, a messaging app, passed the phone ID to eight companies. It sent the phone's ZIP code, along with the user's age and gender, to two of them.