JWT

WHITE PAPER

PRIVACY IN THE DIGITAL AGE

JULY 2008

EXECUTIVE SUMMARY

Citizens of modern societies live in a world of digital data, generating an information trail as they e-mail, shop with loyalty cards, surf the Web, make wireless calls. In response, cautious consumers, watchdog groups and governing bodies are raising alarms about the Orwellian implications. As technology gets ever more powerful and sophisticated, the issue of digital privacy is rapidly coming to the fore.

Key Questions

- What are the privacy issues that are top of mind when discussing search engines, ISPs and Web giants like AOL and Microsoft? What steps are governments taking to regulate and control their activities?
- Just how concerned are consumers about their digital privacy? Does "radical transparency" equate to more lax attitudes toward privacy in general?
- What new technologies are likely to raise additional privacy concerns?
- How can marketers best allay privacy concerns among their customers?

Key Findings

Online, we have little control over all kinds of information we might prefer the public not to have at their fingertips—from what our home looks like (see Google Street View) to our age (see Spock.com). The Internet also makes it easy to embarrass, shame and hurt people, and this seems to be a growing phenomenon.

In the past year, acquisitions have concentrated digital data into the hands of the Web giants. In addition, Internet service providers have started partnering with companies like Phorm and NebuAd in order to record and analyze customer activity. Ad targeting is hot, and the race is on to see who can nail it. To calm fears about privacy implications and to avoid regulation, many of the big players are following voluntary guidelines and initiating consumer education efforts.

A majority of consumers are not comfortable being tracked online, although not many take active steps to protect their privacy. This may change as more people become better informed about online privacy issues.

In the U.S., the dominant attitude is that companies should self-regulate and that consumers in turn should be allowed to opt out; the Federal Trade Commission recently proposed voluntary guidelines covering behavioral targeting. Europe is much less laissez-faire: The prevailing standard is generally "opt in" for consumers, and the EU has been researching legislative and technological solutions for enhancing digital privacy.

As privacy becomes an increasingly high-profile issue, it will be imperative for marketers and tech giants to become more transparent and to put maximum control into consumers' hands, easing the "creepy" factor and enhancing choice.

Back in 1999—in digital-evolution terms, a couple of months after Google launched—Sun Microsystems CEO Scott McNealy was asked whether a new Sun technology would have privacy safeguards. "You have zero privacy anyway—get over it," he famously snapped back.

The Millennial generation has gotten over it and then some, embracing the ethos of radical transparency—ditching the locked diary of yore for blogs or Bebo profiles that document every detail of their lives. By extension, many of today's twentysomethings don't mind being watched by marketers (a recent Harris poll found that almost half of American Millennials are comfortable with being tracked online for ad-targeting purposes, compared with a third of Baby Boomers). But cautious consumers, watchdog groups and governing bodies are raising alarms that new technologies could open the digital doors to a Big Brother society.

"If George Orwell had lived in the Internet age, he could have painted a grim picture of how Web monitoring could be used to promote authoritarianism," warned *The New York Times*' Adam Cohen in a recent opinion column. *The Economist* sounded a similar note last September: "These days, data about people's whereabouts, purchases, behaviour and personal lives are gathered, stored and shared on a scale that no dictator of the old school ever thought possible."

The most apt analogy is not Big Brother but, as New York University journalism professor Adam L. Penenberg writes in MediaPost, "a series of little brothers—your Googles, DoubleClicks and ISPs; the credit-rating agencies; social networks like MySpace and Facebook; and marketers who want to know everything about you."

As technology gets more powerful and more sophisticated—along with the ways in which consumers and marketers are using the tools available to them—the issue of digital privacy is fast coming to the fore.

Citizens of modern societies live in a world of digital data—many of the details of our lives (mundane and juicy alike) are contained within our text messages, our e-mail, our online footprints; they are hinted at in the Web searches that Google and others archive, and listed in public records available online; every time we use a credit card or a store loyalty card we reveal where we are and who we are; a growing web of surveillance cameras captures us on digital video, and our homes may be seen on Google Street View; radio frequency ID (RFID) tags embedded in everything from library books to passports can also track our movements.

"It is virtually impossible to go through life in a Western democracy without leaving an information trail behind," note Southampton University professors Kieron O'Hara and Nigel Shadbolt in their recent book, *The Spy in the Coffee Machine: (The End of Privacy as We Know It).*

Sure, the fact that all this personal data is stored, sorted and possibly scrutinized by authorities and big corporations could put us on a dark, Orwellian path, but there's also a major upside to these technologies. They can be empowering, time-saving, indispensable to 21st-century life. GPS-equipped mobile phones allow people to be quickly found in emergencies; RFID tags could, for example, be embedded in guns to make them trackable, or in refrigerators to warn caretakers when shut-ins are low on food; and, of course, the ability to track online activity and target ads accordingly has helped to foster a Web filled with free content.

In the academic world, the field of "reality mining"—studying human behavior by analyzing patterns in the digital record transmitted by mobile phones and other portable devices—has potential applications that range from better managing traffic systems to halting the spread of lethal viruses like SARS. "Suddenly we have the ability to know what is happening with the mass of humanity and adapt society to accommodate the trends we can detect, and make society work better," MIT professor Sandy Pentland told *BusinessWeek* recently. A current MIT project is using reality mining to explore the dynamics of individual and group behavior.

Outside of academia, a range of marketers, tech startups, Web portals and others are learning how to leverage data mining. One of the primary goals is behavioral targeting—directing communications at people based on their consumer profile—a practice that is rising up the radar of both wary consumers and regulators.

This white paper describes the digital dossiers that search engines, ISPs and Web giants like AOL and Microsoft are compiling, as well as recent efforts to regulate these activities. It also explores just how concerned consumers really are about their digital privacy and considers two evolving technologies that are stirring new privacy fears. First, a look at how our digital footprints are expanding, slowly changing our expectations of privacy.

FOLLOWING YOUR DIGITAL FOOTPRINT

In the recent past, it's become clear that embracing radical transparency can have radical consequences, and not in a good way. (Earlier this year, for example, the mayor of a small town in Oregon was voted out of office after a photo of her posing in underwear on MySpace came to public notice.) It's also becoming increasingly clear that in a world of easy digital dissemination, we don't have much control over compromising information, as well as all kinds of stuff we'd prefer the general public not to know, from what our home looks like to how much money we make.

Hong Kong pop star Edison Chen and his many conquests learned this the hard way. Chen had a trove of X-rated photos of himself and various well-known actresses and singers on his laptop; when he took the machine in for repair, the photos were downloaded, and in early 2008, someone started rolling them out online—setting off a scandal that consumed China and put the careers of Chen and the women involved on the line.

The Web is incredibly efficient at making once-private data instantly available to the world (at least the plugged-in world), and while the offending material may be quickly taken down, people have likely already captured and saved it. The Internet certainly makes it easy to embarrass, shame and hurt people—and this seems to be a growing phenomenon.

The college gossip site Juicy Campus, which launched in 2007, has stirred up controversy across American campuses by allowing anyone to post anonymous gossip about fellow students—"a dorm bathroom wall writ large," as *The New York Times* puts it. And *Newsweek* reports that "Already dozens of Web sites exist solely to help those who would shame others." Among them are sites devoted to slamming former love interests (e.g., neverdateher.com) and bad neighbors (rottenneighbor.com, which incorporates Google Maps to show exactly where the offending folks live); sites such as hollabackNYC.com encourage people to upload camera phone photos of public bad behavior.

Dissing exes online has become a new way to not just vent but also spew venom. *The New York Times* points to a YouTube video made by a bitter ex-wife who tells the viewer that she found a stash of her husband's Viagra and porn (the man is named and seen in photos); another woman put a link on her blog to her ex-husband's new Match.com profile ("I've definitely had to adjust to giving up my privacy," the guy told the *Times*).

Online shaming can also translate as digital bullying or taunting. A Canadian teen gained online infamy after filming himself awkwardly acting out a scene from the movie *Star Wars* with an improvised light saber; he left the footage in his school's TV studio, where it was later found by students who posted it online. It become a viral hit, and the boy soon went into therapy.

While the teen's family settled out of court with the students responsible, "Online shaming can be permanent, a digital scarlet letter that is connected to people for life," observed law professor Daniel Solove, author of *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*, on washingtonpost.com.

Web content that others post about us is just one component of our so-called passive digital footprint; the rest is made up of data such as records of home sales, address listings, mentions in the media or alumni updates, to name just a few examples.

We're at the mercy of whatever information the government or data-collection agencies decide to post to the Web. For example, in late April the Italian tax office posted online the name, address, income and tax status of every citizen, a move it said would promote transparency. Not surprisingly, this generated much outcry before the country's privacy watchdog complained and the site was taken down.

Much of this information has always been public but generally stayed out of sight and mind in dusty government archives. Says Daniel Solove in his book *The Digital Person:* "Our personal information in public records remained private because it was a needle in a haystack, and usually nobody would take the time to try to find it. This privacy is rapidly disappearing as access to information is increasing."

By the same token, anyone with your street address could take the time to drive by your home if truly curious—but Google's Street View feature makes it almost instantly possible to check out an address in an urban area. Providing 360-degree ground-level views of a city's streets, the service launched in May 2007 in the U.S. and currently covers more than 40 of the country's metropolitan areas. There are many privacy implications: Google's cameras have captured people going into porn shops, for example. In the U.S., it hasn't yet stirred up much fuss, however, beyond a recent lawsuit in which a Pittsburgh couple sued Google for invasion of privacy.

It remains to be seen how the service will be received in countries where people may have greater expectations of privacy—Google has said it intends for Street View to become worldwide. It is soon to add several Canadian and Australian cities, and has agreed in both cases to blur faces and license plates due to privacy objections.

Most of us have Googled others, and perhaps also checked Facebook, Flickr, Amazon wish lists or LinkedIn for further info. Now a new group of startups is aggregating all that information; in effect, they are search engines tailored to the task of people search, a one-stop shop that collects the clues people leave about their lives on the aforementioned sites and others.

The goal is to type a name or e-mail into the search bar and get back age, location, occupation and in some cases a photo and a list of the social networking sites to which the person belongs. (How do they do it? While Facebook, LinkedIn and others generally don't share users' e-mail addresses with outside parties, they do offer search based on e-mail address; for sites that don't, the people-search engines use proprietary technology.)

Many of these sites are still in beta, and thus far the results have been hit or miss. When they work as advertised, it can be disconcerting when searching for oneself. Try it on Wink ("Find a person and get info about their school, work, phone number and more") or on RapLeaf.com, which advises on its FAQ: "We encourage you to look up people's Rapleaf reputation before transacting, hiring, or even interacting with them." Rapleaf also purports that it helps people to manage their privacy by allowing them to edit what comes up on the site when someone searches for their name.

"We realized that we're in a very interesting state in the market where there's a lot of people-related information out there; people have their bio pages under 'about me,' people have their MySpace page and so on," says Jaideep Singh, CEO of Spock.com, a people-search engine that aims to index biographical information the way Google indexes Web pages. Its business model is based on targeted advertising, as it is with most similar sites.

In addition to these sophisticated sites, of course, there are the many plain old people-search databases intended to supplant the White Pages. In the old days, one could just decline to be listed in the book. Today, you can petition to have personal data removed, a difficult task given the number of database sites and the speed with which new listings can pop up.

Naturally, there's a whole industry in data suppression, for both individuals and companies—businesses like ReputationDefender, RemoveYourName.com and DefendMyName monitor negative Web references for their clients and get them removed or at least buried. It's far from fail-safe, however:

ReputationDefender's FAQ warns that it cannot guarantee its "Destroy" results, cautioning that "We work very hard for our clients, but our job is hard." They can't just delete information published on other Web sites, they can only automate the process of requesting that a page get removed.

Even if pages are taken down, wiping the slate clean is almost impossible. Google maintains an archive of recent content in its cache, and the Internet Archive claims to have archived 85 billion Web pages dating back to 1996 (searchable through its "Wayback Machine" at archive.org).

THE DIGITAL DOSSIER AND BEHAVIORAL TARGETING

"Individuals tend to forget that much of what they do online is being recorded," says privacy and security consultant Rob Douglas in *Computerworld*. "This collection of information is all done behind the scenes; it's not visualized when individuals are using their computers."

As you surf, browsers save cookies on your computer—user-specific pieces of information that Web servers will later access to remember your user name or what was in your shopping cart, for example. Cookies track what you do on a specific site and can also log what you do elsewhere. Google and others can couple the information they get from cookies and browsers (which may point to a workplace or location, and in some cases reveal your name and e-mail address) with the searches you perform.

In the past year, acquisitions have concentrated this digital data into the hands of the major Web players, which had been seeking to combine the information they collect with the data about user behavior that ad networks gather. Google completed its acquisition of ad sales management firm DoubleClick in March, and in 2007 Microsoft bought aQuantive (which owns the ad delivery company Atlas) and AOL acquired Tacoda, which provides behavioral targeting technology. In April Yahoo unveiled Amp, an ad-publishing platform that uses technology gained through previous acquisitions; the company noted that Amp will "provide a suite of tools that easily allows precise geographic, demographic and interest-based targeting across a vast network."

Targeting is hot, and the race is on to see who can nail it. "Behavioral targeting" is the practice of using data collected online to target ads to the right Web surfers—a Boomer woman is far more likely to see Botox promotions than Grand Theft Auto banners, for example. "Once personal data becomes currency," Debra Goldman sagely predicted in a 1999 *Adweek* column, "all the best privileges and perks will go to those who sell it."

Potentially, these data collections—or digital dossiers, as they're often called—could reveal your political preferences, sexual preferences, underwear preferences. Companies say they take pains to ensure that targeting data is not linked with personally identifiable information. Privacy advocates worry, however, about the implications of these data archives. For example, the government can subpoena information or the information could be lost or stolen.

Users can delete their cookies or block them altogether, but since cookies were designed to make Web surfing easier and more seamless, going without them makes it more (if not very) difficult. There are also ways to surf anonymously, with software like Anonymizer Anonymous Surfing, via sites like the-cloak.com and with the Firefox browser extension TrackMeNot. Declare TrackMeNot's creators, Daniel C. Howe and Helen Nissenbaum: "Because the Web has grown into such a crucial repository of information and our search behaviors profoundly reflect who we are, what we care about, and how we live our lives, there is reason to feel they should be off-limits to arbitrary surveillance."

As targeting becomes more high-profile, its practitioners are hoping to stem such sentiments. In recent months AOL has run an online campaign to educate consumers about behavioral targeting. The campaign explains cookies and targeting by way of an animated penguin who visits AnchovyGourmet.com, then later sees fish-themed ads when he visits another site. The final message allows viewers to click for more info about online advertising and privacy choices. In mid-April, however, AOL's Jules Polonetsky noted at a conference that only about 1 percent of users had clicked through on a banner ad leading to the campaign.

Google is taking a multimedia approach to a range of privacy issues—last fall it set up a "Google Privacy Channel" on YouTube that offers two dozen videos explaining the company's privacy policy (including French, German and Spanish versions) and everything from Street View to unlisting phone numbers.

Meanwhile, the search engine Ask.com, which has just a 5 percent share of the U.S. market, introduced a privacy feature last December intended to differentiate the service from competitors. AskEraser, which is a button on the home page, can be turned on or off with a click and allows people to conduct searches that will not be tracked.

At the same time that the major Web players are ramping up their targeting technologies, Internet service providers are getting into the act as new technologies present the possibility of an additional revenue stream. A crop of companies including Phorm, NebuAd, Front Porch and Adzilla has developed hardware that, once installed on the ISP networks, record and analyze users' activity—basically tracking every click they make. ISP-level tracking may well set off what *New York Times* technology blogger Saul Hansell is calling "the mother of all privacy battles."

Explains NebuAd chairman and CEO Robert Dykes, former chief financial officer at Symantec: "While portals such as Yahoo may collect information on a fraction of user surfing behavior, Web-wide behavioral advertising companies are able to observe most of a user's surfing behavior."

The big question is whether the information collected is personally identifiable. Phorm and others argue that it's not—Phorm doesn't store an IP address or browsing history but rather sets a cookie on a user's browser that gets refined as data accumulates over time. Phorm and NebuAd both say they don't keep tabs on visits to sites related to sensitive topics (health, sex, etc.), and they don't look at e-mails, banking sessions or social networking posts. The companies are less interested in individuals than in audience segments.

In fact, the companies argue that they offer greater privacy protection than existing means of behavioral targeting. Their hardware is programmed to look only at behavior that will slot the user into a consumer profile, and once a profile has been created, Web surfing history is said to be discarded—this then adds up to less information stored for less time than is the case with search engines.

"This is the holy grail for advertisers—privacy-friendly but targeted," declares Marc Burgess, the head of technology at Phorm, a company with offices in London and New York.

It's certainly an appealing proposition for marketers. Dykes says these companies can "define more meaningful audience segments" than other Web players. And user profiles can be developed more quickly, he claims, allowing advertisers to know what the consumer is interested in right now. (The business model has participating Web sites host the relevant ads while ISPs get a percentage of the ad sales, as the middleman in the transaction.)

The challenge is to persuade consumers that the technology is privacy friendly, and in the U.K., that has been proving difficult. Phorm's plans to operate in the country (its first anywhere) were greeted with protest earlier this year, with blogs such as BadPhorm and Dephormation urging boycotts of the ISPs looking to partner with the company. In March, Web pioneer Sir Tim Berners-Lee told BBC News he would switch his ISP if it started using a tracking system such as Phorm.

Currently, BT Broadband is expected to start a trial in which customers must give consent before they are tracked; Carphone Warehouse had said it will also use an opt-in system. The country's other major ISP, Virgin Media, was assessing the technology.

In the U.S., there have been few alarmist headlines thus far, even though an estimated 100,000 Americans are tracked by such services. A recent report by two public interest groups named five companies that use the services of NebuAd, a company similar to Phorm. (NebuAd itself won't say how many or which ISPs it works with.) The lack of fuss is largely due to the fact that these companies have slipped in under the radar—customers are notified but often within the small print of customer service agreements.

When Charter Communications, a large cable operator, tried a more transparent approach earlier this year, it encountered significant obstacles. After Charter sent letters to selected high-speed Internet customers informing them that it planned to test NebuAd, customers complained and two congressmen urged Charter to abandon the plan. It's currently on hold.

It remains to be seen whether Charter customers react with anywhere near the fury that met Phorm in the U.K. and whether Phorm's British reception proves to be a sign of widespread consumer and media wariness. If ISP tracking rises up the media radar in the U.S., will Americans care enough to opt out? Phorm is said to have talked to ISPs around the globe, and its adoption depends in large part on how Internet users worldwide regard the privacy implications.

Ultimately, despite the assurances of privacy protection, the gut-level question remains that posed by *The New York Times*' Hansell: "How comfortable are we in allowing private companies to snoop on us so long as they promise to forget all the juicy bits?"

DO WE GIVE A DAMN?

Whether Phorm's rocky debut in the U.K. was due to cultural factors or just a perfect storm of other elements is hard to say (unlike NebuAd, Phorm is publicly traded and, in an old incarnation, once provided spyware-type applications). But at least some suggest it's the former. "Americans are used to having their personal data bought and sold in a way that is entirely unlawful within Europe," Phorm critic Richard Clayton of the Foundation for Information Policy Research told the Associated Press in April.

Clearly, privacy is a concept that varies widely by culture. For example, while Italians were largely furious about having their tax records posted online, Norwegians have been accustomed to seeing tax data posted on the Web since 2002 (before that, paper records had been open for more than a century).

Notions about privacy have also changed in the recent past, a result of factors ranging from the advent of radical transparency to greater acceptance of government and employee monitoring in the wake of 9/11 and corporate scandals such as Enron. In 1994, 65 percent of Americans who participated in a

Harris Interactive phone survey said it was "extremely important" that they not be monitored at work; in a Pew Internet & American Life survey conducted in late 2006, just 28 percent said it was "very important" they not be monitored.

Less dramatically, 49 percent of adults in the '94 survey felt it was "extremely important" that people in social and work settings not ask highly personal questions; that percentage slipped to 42 percent in the 2006 Pew survey.

Most of the research into attitudes toward online privacy and behavioral tracking has been done in the U.S., and it seems to show that not surprisingly, older generations are more protective of their online privacy. A Harris Interactive survey conducted in March asked respondents whether they were comfortable with being tracked online for the purpose of targeted ads; the question noted that services like free e-mail and search are made possible by online advertising. Younger respondents were more amenable, although fewer than half of Millennials and Gen-Xers said they would be comfortable (49 percent and 45 percent, respectively). Only about one-third of Boomers (34 percent) and respondents 63-plus (31 percent) said they would be comfortable.

Overall, 59 percent in the 1994 Harris survey said they were not comfortable with Web tracking. A study of American adults conducted in February by TNS on behalf of consumer privacy organization TRUSTe echoed the Harris results: 57 percent said they were not comfortable with advertisers using their browsing history to serve relevant ads, even if that information is anonymous.

With a solid majority uncomfortable with tracking in this survey and similar ones, it's clear that radical transparency does not equate to lax attitudes toward privacy in general. "We worry about cookies despite many of us voluntarily becoming open books via sites like MySpace, Facebook and LinkedIn, which are designed to share personal information that until recently would have been considered confidential," writes L. Gordon Crovitz, former publisher of *The Wall Street Journal*, in a May issue of the newspaper.

Still, expressing worry and discomfort is a long way from taking action. "After almost a decade of exploring the issue of privacy, I've come to the realization that most Americans simply don't care," wrote Adam Penenberg in MediaPost recently. "Sure, they say they do. … But most aren't concerned enough to do anything about it."

What if it were easier to do something about it? A large minority of respondents in the TRUSTe survey (42 percent) said they would sign up for a "do not track" type of online registry—an idea that U.S. privacy advocates are pushing—even if that means seeing more ads that are less relevant to their interests.

When it comes to concern about online footprints, a Pew Internet & American Life survey conducted in late 2006 divides Internet users into four points of view:

- "Unfazed and inactive," the largest group at 43 percent of respondents, don't worry about what's out there and take no steps to limit information.
- "Worried by the wayside," about one- fifth of Internet users, have some concerns but take no proactive steps.
- "Confident creatives," the smallest group, actively upload content but take some steps to limit personal information.
- The "concerned and careful," roughly one-fifth of the U.S. Internet population, take proactive measures to limit their footprint.

Privacy advocates argue that consumers have remained relatively blasé about Internet privacy issues only because they're in the dark about just how much data gathering is done. Online tracking by marketers, said the Center for Digital Democracy's Jeffrey Chester at a recent privacy forum, is "a secret for the vast majority of people here in the United States, Europe and elsewhere." Interactive online advertising, he says, is "a virtually invisible, stealth system."

In addition, Web site privacy policies don't exactly make for zippy reading, so few people are well-informed about what kind of privacy they can expect. *Newsweek* reports that when a 2006 study at Carnegie Mellon University asked Facebook users about the site's privacy policy, 70 percent of answers were incorrect. And more than half of Facebook users who used the default privacy settings vastly underestimated how many people could view at least some portion of their profile, figuring it was somewhere in the tens of thousands or fewer, while it was actually in the millions.

Also, according to the Pew survey, fewer than half of Americans have checked out their online footprint (47 percent)—although this is way up from 22 percent in a 2002 survey. Almost three-quarters of those who have searched for their own name said they'd done so just once or twice; one in five said they were surprised by how much information they have found about themselves online.

Thus far, Facebook has served as a bellwether of sorts when it comes to privacy boundaries. Its Newsfeed feature initially ruffled feathers—many members didn't like seeing their newly single status, for example, broadcast to their network—but today most consider it an integral part of the site. Last November, however, Facebook made a now-infamous misstep into the privacy red zone when it introduced Beacon, which reports back to a user's network the purchases that he or she makes on a few dozen participating Web sites. Political advocacy group Moveon.org led a revolt, and Facebook backed off, increasing opt-in provisions.

REGULATORS IN THE COOKIE JAR

Writing about the widespread tendency to see "something potentially creepy" in the use of cookies online, L. Gordon Crovitz warns in *The Wall Street Journal*: "Unless people can be reassured, there is a real risk that someday soon we'll find the untested hands of regulators in the cookie jar." The anti-regulation argument is that "if politicians restrict it unthinkingly, advertising relevance will diminish, and spam will have a renaissance," as Interactive Advertising Bureau president Randall Rothenberg told Crovitz.

There's little evidence to support their fears in the U.S., however, where the Federal Trade Commission recently proposed self-regulation guidelines for behavioral targeting. The U.S. has almost no national laws governing what information businesses can collect about people; despite the best efforts of advocacy groups, the dominant attitude is that companies should voluntarily comply with privacy standards and that consumers in turn are responsible for staying informed.

Europe is much less laissez-faire: The EU has been researching policy options to enhance privacy and recently kicked off a research effort to develop better ways for people to control digital privacy over their lifetime. While the prevailing standard in the EU is generally "opt in" (consumers give consent before any privacy-compromising activities take place), in the U.S. it's more "opt out" (the activity is automatic, but people can refuse participation if they choose).

Last fall, as the U.S. Federal Trade Commission was considering the issue of behavioral targeting, a coalition of nine privacy groups petitioned the U.S. government to start a do-not-track list for those who object to behavioral targeting, similar to the Do Not Call list maintained by the FTC. The coalition also wants Internet ads to disclose whether they are using behavioral tracking and companies to show consumers the profiles they are building about them, upon request.

When the FTC issued its proposed privacy principles late last year, the commission emphasized that targeting provides benefits to consumers (in terms of free content and more relevant advertising) but noted that "this practice is largely invisible and unknown to consumers." A period for public comment ended in mid-April, and formal guidelines may follow.

The principles include allowing consumers to opt out of such advertising, getting consumers' consent before targeting ads based on "sensitive" data (e.g., pertaining to health conditions or sexual orientation), disclosing to users how their information will be used, taking steps to safeguard user information and not sharing personally identifiable data without a user's consent. It doesn't specify how much time companies can keep the data they collect—a major issue in the EU—only advising that data be held "as long as is necessary to fulfill a legitimate business or law enforcement need." Disclosure about behavioral advertising must take the form of "a clear, concise, consumer-friendly, and prominent statement" that makes consumers aware their activities are being tracked and makes clear they can opt out.

Notably, the Harris poll that asked respondents how comfortable they are being tracked online also asked how comfortable they would be if Web sites followed four basic privacy/security protocols that were based on the FTC's proposals; this time, fewer than half (45 percent) said they would not be comfortable, a drop of 14 points from the original question.

Some of the FTC's proposals are currently followed by members of the Network Advertising Initiative, which counts about a dozen major U.S.-based ad networks among its members. In April, the NAI proposed several updates to its self-regulatory guidelines, including banning behavioral targeting at users inferred to be 13 and under; it also compiled a list of searches that companies should not track, pertaining to health (such as HIV/AIDS status, cancer status and psychiatric conditions) and other very personal issues (such as sexual behavior and orientation). The NAI Web site allows consumers to opt out of behavioral advertising from member ad networks.

The problem that privacy advocates have with opt-out is that it almost always requires work and some smarts. "Only if consumers are strongly interested, extremely literate, well-informed and highly skilled can they negotiate the opaque, inconsistent morass of opt-out procedures," noted a brief filed by the Consumer Federation of America in response to the FTC's proposals.

Still, opt-out itself is a fairly recent concession, where it exists at all; for instance, Microsoft began offering an opt-out for targeted ads in mid-2007. (Microsoft also allows users to opt in if they want the company to combine personally identifiable data with data on Web activities; the advantage—likely dubious to most—would be discount offers.)

There are a few signs that digital privacy may become a bigger regulatory issue in the U.S. Democratic Congressman Edward Markey and Republican Joe Barton, who together founded the Congressional Privacy Caucus, successfully put pressure on Charter to freeze its NebuAd plans. Barton is questioning Google about its privacy policies in the wake of the DoubleClick acquisition. And the Senate Commerce Committee has scheduled a hearing on the privacy implications of online advertising for mid-July.

The European Union has been much more concerned than American authorities about privacy issues, especially when it comes to data retention by search engines. In April, the Article 29 Working Party, which advises the EU on privacy issues, issued a recommendation that search engines discard personal search data after a maximum of six months (or make them completely anonymous) and allow consumers to see the data collected about them. It also recommended that search engines be required to link to their privacy policies on their home page (which Google does not do) and with search results.

The EU is expected to follow the commission's guidance when drafting rules covering online privacy. If it does, it is likely that Google would have to implement the changes system wide, not just for European users. Currently, Google and Microsoft hold on to the data for up to 18 months (recently reduced from 24 to placate privacy advocates); Yahoo keeps it for 13 months.

Seeking solutions to privacy protection on the tech end as well, the EU is providing €10 million ($15.7 million) to help fund a three-year initiative led by IBM's Zurich Research Laboratory that's seeking ways of enhancing the security of personal data. The project, which kicked off in March, aims to create an Identity Management System that would give the user "an overview of which personal data he or she uses, when, where and how" and allow the person to define default privacy settings and preferences for a variety of applications, including social networks and virtual communities. A longer-term goal is to find ways to maintain lifelong control over one's privacy.

This will be no easy task: "Resolving these issues requires substantial progress in many underlying technologies," notes the home page for the PrimeLife project (short for Privacy and Identity Management in Europe for Life). PrimeLife's multidisciplinary consortium includes partners from several European academic and research institutions as well as Brown University in the U.S.

PRIVACY'S NEXT FRONTIERS

Consumers generate digital data well beyond their desktops and laptops, and fast-evolving technologies, such as location-trackers on mobile devices, appear likely to become new fronts in the privacy skirmish between consumers, marketers and regulators.

Wireless carriers could well be caught in the center of the crossfire. Thus far, most have done little with their call data, partly for fear of a privacy backlash and partly because lucrative opportunities are only now arising. With the advent of GPS-equipped phones, they have begun partnering with marketers that want to target people based on location (as well as, in some cases, user profiles generated from calling patterns). Measurement services like Nielsen Mobile have recently begun working with carriers and manufacturers to install meters in smartphones (participants get paid nominal amounts if they opt in), generating "a comprehensive array of metrics on actual consumer behavior," according to Nielsen.

As more consumers adopt smartphones—using them to write e-mail, shop online, etc.—the carriers and third-party partners will have access to a well of valuable data that marketers would likely pay handsomely to mine.

Meanwhile, new location-tracking services for mobile phone users are opening up a range of possibilities for both users and marketers. "Advertisers are eager to seize on the popularity of location-based services that allow phone subscribers to map their whereabouts and get localized content," reported *The Chicago Tribune* in April. Thus far the ideas stick to opt-in systems for consumers rather than unsolicited messages, the newspaper notes—people could seek out local promotions by providing a postal code, for example.

One of the first applications on the market is the social-mapping service, allowing people to track where their friends are more or less in real time via a map on their mobile screen. It's radical transparency in motion, and aimed squarely at the Millennial generation. Go much beyond this market and not many people are likely to relish the thought of their network knowing where they are at all times.

Loopt is a California social-mapping company (led by a 22-year-old, naturally) that relies on GPS technology, which is required by law in all new American phones. U.S. carrier Sprint Nextel says it has signed up hundreds of thousands of users since it started offering Loopt to subscribers in July 2007. Verizon Wireless began offering Loopt this past June. And Loopt will also be available as an app for the latest iPhone.

In the U.S., Helio, a mobile virtual-network operator, offers a similar feature; AT&T has said it plans to offer such a service. A Yahoo service that combines location tracking with instant messaging will soon be available for mobile phones.

Sniff is a service that works in conjunction with Facebook (Sniff stands for Social Network Integrated Friend Finder) to allow networks of people to find each other, with users charged by the "sniff." It launched in Sweden (where Sniff claims more than 80,000 users) and Denmark, and debuted in the U.K. in June; there are plans to roll out in the U.S., Canada and France in the coming months. Sniff, which can be accessed from Facebook or mobile phone, doesn't rely on GPS but rather location information from carrier base stations.

A Japanese wireless carrier targets parents with GPS-enabled "Kids' Phones." And GeoSolutions BV in Amsterdam plans to make a Loopt-like feature available through a Chinese wireless carrier in time for the Beijing Olympics; currently it offers a downloadable application that allows users to track others using the GyPSii service.

In the U.S., the companies have moved cautiously, wary about a privacy backlash and abuses of the system by marketers or criminals. "When it gets to privacy, that's quite frankly an area where we can't afford to make any mistakes," Ryan Hughes, a vice president at Verizon Wireless, said in an interview in *The Wall Street Journal* in March.

Loopt subscribers can see only friends in their network, and they can turn off tracking for specific friends or for all contacts. To sign up, customers must scroll through pages of disclaimers and privacy notices. Sniff assures that only those who consent will be tracked, that users can specify which specific friends can "sniff" them, and that users can make themselves invisible to the network. It sends multiple confirmation messages to new users to remind them they have joined the network and what their permission levels are.

Loopt has a privacy officer, who is discussing the company's privacy policies with U.S. government officials as well as advocacy groups, although there's no sign yet of regulations that would cover location tracking. Eager to ensure that this remains the case, a trade group for wireless carriers, CTIA-The Wireless Association, introduced privacy standards for location-based services in April.

Regulation is likely to be instituted in at least some parts of the world, however, given the issues that can arise—for example, will companies be required to turn over location information to authorities looking for suspects? And at least one U.S. Congressman is tuned in to the topic of location tracking: "There has to be a national debate about what the privacy implications are," Edward J. Markey told *The Wall Street Journal.*

RFID TECHNOLOGY AND THE PRIVACY DEBATE

Radio frequency identification (RFID) technology, which combines computer chips with tiny radio antennas that send information back to databases, has until now mainly served to help retailers track inventory. As the price per tag drops, the expectation is that they will get embedded in an array of consumer products, replacing the barcode and allowing retailers and police to track items beyond the store. The tags will likely be embedded in "smart homes" as well: A refrigerator could warn its owner that milk is needed, a microwave could heat a frozen meal without instruction.

Analysts estimate that within the decade, the cost per tag could drop below one U.S. cent, making it economically feasible for manufacturers to tag almost everything. The implications: "Once a tagged item is associated with a particular individual, personally identifiable information can be obtained and then aggregated to develop a profile," according to a 2005 U.S. Government Accountability Office report. (Unlike barcodes, RFID tags each carry unique numbers.)

For privacy advocates, the possibilities are frightening: Unbeknownst to consumers, companies could "rifle through people's pockets, purses, suitcases, briefcases, luggage—and possibly their kitchens and bedrooms—anytime of the day or night," says FTI Consulting's Mark Rasch, former head of the U.S. Justice Department's computer-crime unit. And, he told the Associated Press, the data collected will be "used in unintended ways by third parties" such as marketers, private investigators and the government.

Indeed, for marketers the possibilities are intriguing. An RFID-equipped fridge, for example, could send signals to the television so that its owners see commercials for foods or categories they prefer. In public places, electronic trackers will likely be able to read tags embedded in people's clothing and accessories and display customized ads or coupons for nearby stores.

The Associated Press reports that IBM got patent approval in 2006 for what it termed "Identification and tracking of persons using RFID-tagged items." One possible use outlined is to collect data about a person in order "to monitor the movement of the person through the store or other areas." Information from RFID tags would be combined with a store's sales records to determine identity. Other corporations have received patents for similar systems or have filed patent applications, including American Express and Procter & Gamble.

The tags are already in use in some library books, passports, employer badges and loyalty cards. And they are embedded in some consumer products; for example, Pfizer puts tags in Viagra bottles in the U.S. as an anti-counterfeiting measure. An RFID pilot project kicked off at a department store in Essen, Germany, last year, with thousands of garments now tagged; the applications are creative—a man trying on a dress shirt may see tips on what to pair with it pop up on a screen in his changing room. (The chips are inside a paper tag that customers or cashiers can easily remove.)

Tags are also being incorporated into mobile phones, allowing people to pay for products with their phones, which they link to a bank account or credit card. In Seoul, McDonald's has been trying out a system in which consumers order and pay via touch-pad menus equipped with RFID readers that link to mobile phones.

The EU has been out in front in efforts to put privacy guidelines in place before the tags proliferate. In February, the European Commission issued a proposed code of conduct for companies that use RFID tags; the principal requirement is that consumers opt in to the technology or chips must be deactivated after items are purchased. Once the EC's proposals are finalized, they serve as a guideline for EU members to enact their own regulations.

Not surprisingly, an industry trade group is advocating for an opt-out rather than opt-in approach. Meanwhile an EU-funded pilot program, the EuroPriSe Project, is investigating ways to create a "privacy seal of approval" that would mimic the way organic or fair trade products are certified.

WHAT IT MEANS

In 2006, the U.K.'s Surveillance Studies Network produced "A Report on the Surveillance Society" for the country's Information Commissioner. Looking 10 years into the future, the authors paint a picture of malls where intelligent billboards target consumers based on the RFID tags in their clothing. Consumers' handheld devices transmit marketing messages tailored to the type of shopping they're doing. Some will pay for goods via a chip implanted in their arm; the incentive to do so will be store discounts and access to VIP lounges. Anti-capitalist activists, meanwhile, will plaster aluminum sheeting and tiny microwave transmitters at store entrances, disrupting the wireless signals that connect to mobile devices.

Are we really less than a decade away from this scenario? The fact is, this might be the tip of the iceberg in terms of our future privacy concessions. "If the short-term benefits of technology are good enough, we tend not to question them," observe O'Hara and Shadbolt in *The Spy in the Coffee Machine*.

Then again, people may well grow more protective of their electronic privacy. Beyond the issues outlined here—mostly areas in which the interests of marketers intersect with privacy concerns—other factors are likely to ratchet up anxiety, notably increased government snooping in a post-9/11 world and the fast-evolving sophistication of identity thieves. And if personal data is seriously compromised in one too many high-profile cases, wariness is sure to become more widespread.

"With the collection and centralisation of such vast amounts of data, the potential for abuse is huge and the safeguards paltry," noted *The Economist* last September, referring to all forms of electronic surveillance and data collection. Just two months later, in fact, the British government lost two CDs containing unencrypted personal and financial data on 25 million citizens.

Holding onto massive amounts of information about what people are doing online is a "ticking privacy time bomb," alleges Marc Rotenberg of the Electronic Privacy Information Center in Washington, D.C.

They may be passive about it, but consumers are already plenty concerned about privacy. In an opinion piece in *The Wall Street Journal*, L. Gordon Crovitz notes one reason that collecting information online seems to worry people more than similar offline activity: "Scholar Joseph Turow has identified a 'culture of suspicion.' People don't understand how the Web works, so fear they are being spied on and manipulated."

Or perhaps people understand all too well—after all, the outside world has never had such power to know what they're doing and thinking. "Tracking on the Internet is like being constantly followed by a private investigator with a dynamic billboard," wrote one poster on a *New York Times* tech blog. "Only worse, because most people probably do more private things on the Internet than they do in their real world neighborhood."

Such sentiments will make it imperative for marketers and tech giants to become transparent and to put maximum control into consumers' hands—ease the "creepy" factor and enhance choice.

At a social media conference in Los Angeles in April, a Yahoo exec advocated allowing users to see behind the scenes of behavioral targeting: "I could envision an icon that appears when you see an ad, and if you were to click through that icon, you would see the data we're leveraging," said Jeff Weiner, head of Yahoo's Network division. He told the crowd: "It's going to be very difficult going forward as an industry to limit users' [access to information]."

The first step is to demystify the technology (for example, explaining how cookies make Web surfing more seamless), help consumers understand the tradeoffs they're making (exchanging personal data for the ability to access free content, and so on) and bring home the benefits of data collection. AOL's campaign is a start, but it needs to find better ways to attract notice.

"We have a solid indication that consumers want us to find a way to get them the advertising that is relevant to them," says Fran Maier, executive director of U.S. consumer privacy organization TRUSTe. "Behavioral targeting is one of the most promising methods, but at the very least, it has to be made more transparent, provide choices and deliver real value."

Providing choices will be essential, and today choice is evolving well beyond opt in or opt out toward "granular control"—allowing users to fine-tune their level of openness. For instance, Facebook recently refined its privacy controls to the point where members can specify whether second- or third-degree contacts can see their profile and who in their network can view content like photographs (in other words, what happens in Vegas stays in Vegas—or at least, among the buddies who were there with you). Navigating granular controls will become second nature to Millennials and Gen-Xers.

Providing options ties into an important factor, one that parents know well: "Citizens will adopt technology when it is both optional and beneficial to them," notes *The Economist*, "but resist it strenuously when it is compulsory, no matter how sensible it may seem."

The authors of the "Surveillance Society" report also foresee a future in which the more fortunate subscribe to personal information management services that monitor their "data shadow." Until then, however, people will need to do it themselves if they are to maintain any control over their reputation, even as those data shadows keep expanding. And for now, a sort of preemptive confessional may become standard for politicians who figure that it's better than waiting for digital evidence to bubble up and spread. After New York Governor Eliot Spitzer resigned amid a scandal involving high-priced hookers, his successor, David A. Paterson, promptly announced that both he and his wife had engaged in affairs during a rough patch in their marriage.

Of course, the wiser path would be to act more ethically in the first place, knowing how easily indiscretions could come to light. Not too likely, but there is a chance we'll become more forgiving, notes Adam Penenberg: "We are all vulnerable to having our secrets shared, and there is little point in pretending to be holier than thou." The upside of seeing our privacy eroded, he says, is "a more tolerant, less judgmental society."

JWT

466 Lexington Avenue
New York, NY 10017
www.jwt.com
www.jwtintelligence.com

WHITE PAPER

Written by	Marian Berelowitz
Editor-in-Chief	Ann M. Mack
Associate Editor	Lois Saldana
Copyeditor	Patty Orsini
Proofreader	Katerina Petinos
Design	Paris Tempo Productions

CONTACT:
Ann M. Mack
Director of Trendspotting
JWT Worldwide
212-210-7378
ann.mack@jwt.com

ABOUT JWT: *JWT, which celebrates its 144th anniversary this year, ranks as the largest advertising agency brand in the U.S. and as the fourth-largest full-service network in the world. It was the first agency to be associated with anthropology and the study of consumer behavior. Its parent company is WPP.*