Mapping, and Sharing, the Consumer Genome

By NATASHA SINGER  JUNE 16, 2012

IT knows who you are. It knows where you live. It knows what you do.

It peers deeper into American life than the F.B.I. or the I.R.S., or those prying digital eyes at Facebook and Google. If you are an American adult, the odds are that it knows things like your age, race, sex, weight, height, marital status, education level, politics, buying habits, household health worries, vacation dreams — and on and on.

Right now in Conway, Ark., north of Little Rock, more than 23,000 computer servers are collecting, collating and analyzing consumer data for a company that, unlike Silicon Valley’s marquee names, rarely makes headlines. It’s called the Acxiom Corporation, and it’s the quiet giant of a multibillion-dollar industry known as database marketing.

Few consumers have ever heard of Acxiom. But analysts say it has amassed the world’s largest commercial database on consumers — and that it wants to know much, much more. Its servers process more than 50 trillion data “transactions” a year. Company executives have said its database contains information about 500 million active consumers worldwide, with about 1,500 data points per person. That includes a majority of adults in the United States.
Such large-scale data mining and analytics — based on information available in public records, consumer surveys and the like — are perfectly legal. Acxiom’s customers have included big banks like Wells Fargo and HSBC, investment services like E*Trade, automakers like Toyota and Ford, department stores like Macy’s — just about any major company looking for insight into its customers.

For Acxiom, based in Little Rock, the setup is lucrative. It posted profit of $77.26 million in its latest fiscal year, on sales of $1.13 billion.

But such profits carry a cost for consumers. Federal authorities say current laws may not be equipped to handle the rapid expansion of an industry whose players often collect and sell sensitive financial and health information yet are nearly invisible to the public. In essence, it’s as if the ore of our data-driven lives were being mined, refined and sold to the highest bidder, usually without our knowledge — by companies that most people rarely even know exist.

**Julie Brill, a member of the Federal Trade Commission**, says she would like data brokers in general to tell the public about the data they collect, how they collect it, whom they share it with and how it is used. “If someone is listed as diabetic or pregnant, what is happening with this information? Where is the information going?” she asks. “We need to figure out what the rules should be as a society.”

Although Acxiom employs a chief privacy officer, Jennifer Barrett Glasgow, she and other executives declined requests to be interviewed for this article, said Ines Rodriguez Gutzmer, director of corporate communications.

In March, however, Ms. Barrett Glasgow endorsed increased industry openness. “It’s not an unreasonable request to have more transparency among data brokers,” she said in an interview with The New York Times. In marketing materials, Acxiom promotes itself as “a global thought leader in addressing consumer privacy issues and earning the public trust.”

But, in interviews, security experts and consumer advocates paint a portrait of a company with practices that privilege corporate clients’ interests over those of
consumers and contradict the company’s stance on transparency. Acxiom’s marketing materials, for example, promote a special security system for clients and associates to encrypt the data they send. Yet cybersecurity experts who examined Acxiom’s Web site for The Times found basic security lapses on an online form for consumers seeking access to their own profiles. (Acxiom says it has fixed the broken link that caused the problem.)

In a fast-changing digital economy, Acxiom is developing even more advanced techniques to mine and refine data. It has recruited talent from Microsoft, Google, Amazon.com and Myspace and is using a powerful, multiplatform approach to predicting consumer behavior that could raise its standing among investors and clients.

Of course, digital marketers already customize pitches to users, based on their past activities. Just think of “cookies,” bits of computer code placed on browsers to keep track of online activity. But Acxiom, analysts say, is pursuing far more comprehensive techniques in an effort to influence consumer decisions. It is integrating what it knows about our offline, online and even mobile selves, creating in-depth behavior portraits in pixilated detail. Its executives have called this approach a “360-degree view” on consumers.

“There’s a lot of players in the digital space trying the same thing,” says Mark Zgutowicz, a Piper Jaffray analyst. “But Acxiom’s advantage is they have a database of offline information that they have been collecting for 40 years and can leverage that expertise in the digital world.”

Yet some prominent privacy advocates worry that such techniques could lead to a new era of consumer profiling.

Jeffrey Chester, executive director of the Center for Digital Democracy, a nonprofit group in Washington, says: “It is Big Brother in Arkansas.”

SCOTT HUGHES, an up-and-coming small-business owner and Facebook denizen, is Acxiom’s ideal consumer. Indeed, it created him.
Mr. Hughes is a fictional character who appeared in an Acxiom investor presentation in 2010. A frequent shopper, he was designed to show the power of Acxiom’s multichannel approach.

In the presentation, he logs on to Facebook and sees that his friend Ella has just become a fan of Bryce Computers, an imaginary electronics retailer and Acxiom client. Ella’s update prompts Mr. Hughes to check out Bryce’s fan page and do some digital window-shopping for a fast inkjet printer.

Such browsing seems innocuous — hardly data mining. But it cues an Acxiom system designed to recognize consumers, remember their actions, classify their behaviors and influence them with tailored marketing.

When Mr. Hughes follows a link to Bryce’s retail site, for example, the system recognizes him from his Facebook activity and shows him a printer to match his interest. He registers on the site, but doesn’t buy the printer right away, so the system tracks him online. Lo and behold, the next morning, while he scans baseball news on ESPN.com, an ad for the printer pops up again.

That evening, he returns to the Bryce site where, the presentation says, “he is instantly recognized” as having registered. It then offers a sweeter deal: a $10 rebate and free shipping.

It’s not a random offer. Acxiom has its own classification system, PersonicX, which assigns consumers to one of 70 detailed socioeconomic clusters and markets to them accordingly. In this situation, it pegs Mr. Hughes as a “savvy single” — meaning he’s in a cluster of mobile, upper-middle-class people who do their banking online, attend pro sports events, are sensitive to prices — and respond to free-shipping offers.

Correctly typecast, Mr. Hughes buys the printer.

But the multichannel system of Acxiom and its online partners is just revving up. Later, it sends him coupons for ink and paper, to be redeemed via his cellphone, and a personalized snail-mail postcard suggesting that he donate his old
printer to a nearby school.

Analysts say companies design these sophisticated ecosystems to prompt consumers to volunteer enough personal data — like their names, e-mail addresses and mobile numbers — so that marketers can offer them customized appeals any time, anywhere.

Still, there is a fine line between customization and stalking. While many people welcome the convenience of personalized offers, others may see the surveillance engines behind them as intrusive or even manipulative.

“If you look at it in cold terms, it seems like they are really out to trick the customer,” says Dave Frankland, the research director for customer intelligence at Forrester Research. “But they are actually in the business of helping marketers make sure that the right people are getting offers they are interested in and therefore establish a relationship with the company.”

DECADES before the Internet as we know it, a businessman named Charles Ward planted the seeds of Acxiom. It was 1969, and Mr. Ward started a data processing company in Conway called Demographics Inc., in part to help the Democratic Party reach voters. In a time when Madison Avenue was deploying one-size-fits-all national ad campaigns, Demographics and its lone computer used public phone books to compile lists for direct mailing of campaign material.

Today, Acxiom maintains its own database on about 190 million individuals and 126 million households in the United States. Separately, it manages customer databases for or works with 47 of the Fortune 100 companies. It also worked with the government after the September 2001 terrorist attacks, providing information about 11 of the 19 hijackers.

To beef up its digital services, Acxiom recently mounted an aggressive hiring campaign. Last July, it named Scott E. Howe, a former corporate vice president for Microsoft’s advertising business group, as C.E.O. Last month, it hired Phil Mui, formerly group product manager for Google Analytics, as its chief product and engineering officer.
In interviews, Mr. Howe has laid out a vision of Acxiom as a new-millennium “data refinery” rather than a data miner. That description posits Acxiom as a nimble provider of customer analytics services, able to compete with Facebook and Google, rather than as a stealth engine of consumer espionage.

Still, the more that information brokers mine powerful consumer data, the more they become attractive targets for hackers — and draw scrutiny from consumer advocates.

This year, Advertising Age ranked Epsilon, another database marketing firm, as the biggest advertising agency in the United States, with Acxiom second. Most people know Epsilon, if they know it at all, because it experienced a major security breach last year, exposing the e-mail addresses of millions of customers of Citibank, JPMorgan Chase, Target, Walgreens and others. In 2003, Acxiom had its own security breaches.

But privacy advocates say they are more troubled by data brokers’ ranking systems, which classify some people as high-value prospects, to be offered marketing deals and discounts regularly, while dismissing others as low-value — known in industry slang as “waste.”

Exclusion from a vacation offer may not matter much, says Pam Dixon, the executive director of the World Privacy Forum, a nonprofit group in San Diego, but if marketing algorithms judge certain people as not worthy of receiving promotions for higher education or health services, they could have a serious impact.

“Over time, that can really turn into a mountain of pathways not offered, not seen and not known about,” Ms. Dixon says.

Until now, database marketers operated largely out of the public eye. Unlike consumer reporting agencies that sell sensitive financial information about people for credit or employment purposes, database marketers aren’t required by law to show consumers their own reports and allow them to correct errors. That may be about to change. This year, the F.T.C. published a report calling for greater transparency among data brokers and asking Congress to give consumers the right
to access information these firms hold about them.

ACXIOM’S Consumer Data Products Catalog offers hundreds of details — called “elements” — that corporate clients can buy about individuals or households, to augment their own marketing databases. Companies can buy data to pinpoint households that are concerned, say, about allergies, diabetes or “senior needs.” Also for sale is information on sizes of home loans and household incomes.

Clients generally buy this data because they want to hold on to their best customers or find new ones — or both.

A bank that wants to sell its best customers additional services, for example, might buy details about those customers’ social media, Web and mobile habits to identify more efficient ways to market to them. Or, says Mr. Frankland at Forrester, a sporting goods chain whose best customers are 25- to 34-year-old men living near mountains or beaches could buy a list of a million other people with the same characteristics. The retailer could hire Acxiom, he says, to manage a campaign aimed at that new group, testing how factors like consumers’ locations or sports preferences affect responses.

But the catalog also offers delicate information that has set off alarm bells among some privacy advocates, who worry about the potential for misuse by third parties that could take aim at vulnerable groups. Such information includes consumers’ interests — derived, the catalog says, “from actual purchases and self-reported surveys” — like “Christian families,” “Dieting/Weight Loss,” “Gaming-Casino,” “Money Seekers” and “Smoking/Tobacco.” Acxiom also sells data about an individual’s race, ethnicity and country of origin. “Our Race model,” the catalog says, “provides information on the major racial category: Caucasians, Hispanics, African-Americans, or Asians.” Competing companies sell similar data.

Acxiom’s data about race or ethnicity is “used for engaging those communities for marketing purposes,” said Ms. Barrett Glasgow, the privacy officer, in an e-mail response to questions.

There may be a legitimate commercial need for some businesses, like ethnic
restaurants, to know the race or ethnicity of consumers, says Joel R. Reidenberg, a privacy expert and a professor at the Fordham Law School.

“At the same time, this is ethnic profiling,” he says. “The people on this list, they are being sold based on their ethnic stereotypes. There is a very strong citizen’s right to have a veto over the commodification of their profile.”

He says the sale of such data is troubling because race coding may be incorrect. And even if a data broker has correct information, a person may not want to be marketed to based on race.

“DO you really know your customers?” Acxiom asks in marketing materials for its shopper recognition system, a program that uses ZIP codes to help retailers confirm consumers’ identities — without asking their permission.

“Simply asking for name and address information poses many challenges: transcription errors, increased checkout time and, worse yet, losing customers who feel that you’re invading their privacy,” Acxiom’s fact sheet explains. In its system, a store clerk need only “capture the shopper’s name from a check or third-party credit card at the point of sale and then ask for the shopper’s ZIP code or telephone number.” With that data Acxiom can identify shoppers within a 10 percent margin of error, it says, enabling stores to reward their best customers with special offers. Other companies offer similar services.

“This is a direct way of circumventing people’s concerns about privacy,” says Mr. Chester of the Center for Digital Democracy.

Ms. Barrett Glasgow of Acxiom says that its program is a “standard practice” among retailers, but that the company encourages its clients to report consumers who wish to opt out.

Acxiom has positioned itself as an industry leader in data privacy, but some of its practices seem to undermine that image. It created the position of chief privacy officer in 1991, well ahead of its rivals. It even offers an online request form, promoted as an easy way for consumers to access information Acxiom collects.
about them.

But the process turned out to be not so user-friendly for a reporter for The Times.

In early May, the reporter decided to request her record from Acxiom, as any consumer might. Before submitting a Social Security number and other personal information, however, she asked for advice from a cybersecurity expert at The Times. The expert examined Acxiom’s Web site and immediately noticed that the online form did not employ a standard encryption protocol — called https — used by sites like Amazon and American Express. When the expert tested the form, using software that captures data sent over the Web, he could clearly see that the sample Social Security number he had submitted had not been encrypted. At that point, the reporter was advised not to request her file, given the risk that the process might expose her personal information.

Later in May, Ashkan Soltani, an independent security researcher and former technologist in identity protection at the F.T.C., also examined Acxiom’s site and came to the same conclusion. “Parts of the site for corporate clients are encrypted,” he says. “But for consumers, who this information is about and who stand the most to lose from data collection, they don’t provide security.”

Ms. Barrett Glasgow says that the form has always been encrypted with https but that on May 11, its security monitoring system detected a “broken redirect link” that allowed unencrypted access. Since then, she says, Acxiom has fixed the link and determined that no unauthorized person had gained access to information sent using the form.

On May 25, the reporter submitted an online request to Acxiom for her file, along with a personal check, sent by Express Mail, for the $5 processing fee. Three weeks later, no response had arrived.

Regulators at the F.T.C. declined to comment on the practices of individual companies. But Jon Leibowitz, the commission chairman, said consumers should have the right to see and correct personal details about them collected and sold by
data aggregators.

After all, he said, “they are the unseen cyberazzi who collect information on all of us.”

A version of this article appears in print on June 17, 2012, on page BU1 of the New York edition with the headline: You For Sale.
SECRET E-SCORES CHART CONSUMERS’ BUYING POWER

By NATASHA SINGER  AUG. 18, 2012

ST. CLOUD, Minn.

AMERICANS are obsessed with their scores. Credit scores, G.P.A.’s, SAT’s, blood pressure and cholesterol levels — you name it.

So here’s a new score to obsess about: the e-score, an online calculation that is assuming an increasingly important, and controversial, role in e-commerce.

These digital scores, known broadly as consumer valuation or buying-power scores, measure our potential value as customers. What’s your e-score? You’ll probably never know. That’s because they are largely invisible to the public. But they are highly valuable to companies that want — or in some cases, don’t want — to have you as their customer.

Online consumer scores are calculated by a handful of start-ups, as well as a few financial services stalwarts, that specialize in the flourishing field of predictive consumer analytics. It is a Google-esque business, one fueled by almost unimaginable amounts of data and powered by complex computer algorithms. The result is a private, digital ranking of American society unlike anything that has come before.

It’s true that credit scores, based on personal credit reports, have been around
for decades. And direct marketing companies have long ranked consumers by their socioeconomic status. But e-scores go further. They can take into account facts like occupation, salary and home value to spending on luxury goods or pet food, and do it all with algorithms that their creators say accurately predict spending.

A growing number of companies, including banks, credit and debit card providers, insurers and online educational institutions are using these scores to choose whom to woo on the Web. These scores can determine whether someone is pitched a platinum credit card or a plain one, a full-service cable plan or none at all. They can determine whether a customer is routed promptly to an attentive service agent or relegated to an overflow call center.

Federal regulators and consumer advocates worry that these scores could eventually put some consumers at a disadvantage, particularly those under financial stress. In effect, they say, the scores could create a new subprime class: people who are bypassed by companies online without even knowing it. Financial institutions, in particular, might avoid people with low scores, reducing those people’s access to home loans, credit cards and insurance.

It might seem strange that one innovator in this sphere has blossomed here in St. Cloud, a world away from the hothouse of Silicon Valley. It is called eBureau, and it develops eScores — its name for custom scoring algorithms — to predict whether someone is likely to become a customer or a money-loser. Gordy Meyer, the founder and chief executive, says his system needs less than a second to size up a consumer and to transmit his or her score to an eBureau client.

“It’s like gambling,” Mr. Meyer says. “It’s a game of odds, when to double down and when to pass.”

Every month, eBureau scores about 20 million American adults on behalf of clients like banks, payday lenders and insurers, looking to buy the names of prospective customers. An eBureau spinoff called TruSignal, also located here, scores about 110 million consumers monthly for advertisers seeking select audiences for online ads. Mr. Meyer says eBureau’s clients use the scores to answer
basic business questions about their potential audience.

“Are they legitimate?” Mr. Meyer asks. “Are they worth pursuing? Are they worth spending money on?” The scores, he adds, are generated without using federally regulated consumer data and are not used to make credit decisions about consumers. (Using regulated credit data for marketing purposes could run afoul of federal law.)

Such assurances aside, consumer value scores have begun to trouble some federal regulators. One of their worries is that these scores, which have spread quietly through American business, measure individuals against one another, using yardsticks that are essentially secret. Another is that the scores could pigeonhole people, limit their financial choices and channel some into predatory loans, they say.

“The scoring is a tool to enable financial institutions to make decisions about financing based on unconventional methods,” says David Vladeck, the director of the bureau of consumer protection at the Federal Trade Commission. “We are troubled by these practices.”

Federal law governs the use of old-fashioned credit scores. Companies must have a legally permissible purpose before checking consumers’ credit reports and must alert them if they are denied credit or insurance based on information in those reports. But the law does not extend to the new valuation scores because they are derived from nontraditional data and promoted for marketing.

Ed Mierzwinski, consumer program director at the United States Public Interest Research Group in Washington, worries that federal laws haven’t kept pace with change in the digital age.

“There’s a nontransparent, opaque scoring system that collects information about you to generate a score — and what your score is results in the offers you get on the Internet,” he says. “In most cases, you don’t know who is collecting the information, you don’t know what predictions they have made about you, or the potential for being denied choice or paying too much.”
ON the ground floor of eBureau’s headquarters are the company’s prized assets: several hundred computer processors that analyze billions of details about consumers every month. EBureau has built a glass enclosure on a raised platform to showcase the machines. From the dimly lit viewing hall, tiny green and blue lights flicker behind glass.

Like many facets of eBureau, the idea of putting the processors on a pedestal came from Mr. Meyer, 51, whose relaxed uniform of jeans and cotton shirts belies the methodological decider underneath.

“In this business, it’s intangible. It’s data through wires,” Mr. Meyer says, walking the perimeter of the enclosure. To help clients relate to his business, he says, he tried to make his data center appear technological, reliable and safe. “We wanted it to feel like it’s a bunker.”

It is actually no coincidence that one of the country’s leading consumer-scoring companies is located here, in this former granite-mining town about a 90-minute drive northwest of Minneapolis. Mr. Meyer, a Minnesota native, learned the scoring principles that underlie eBureau decades ago by working at another local company.

Nearly 30 years ago, he says he took a job as a “lowly number cruncher” at Fingerhut, a general merchandise catalog company based near Minneapolis. A pioneer in customer analytics, Fingerhut specialized in marketing to mid- and low-income customers, offering consumer electronics and other items for sale on monthly installment plans. At the time Mr. Meyer worked there, he says, many Fingerhut customers had little to no credit history.

“Traditional ways to evaluate credit didn’t exist on half of them,” he recalls. “So Fingerhut had to come up with a way to decide who they mailed catalogs to and who they ultimately approved orders to.”

Back then, he says, Fingerhut evaluated creditworthiness based in part on how people filled out order forms. Those who used pens were seen as safer bets than those who used pencils. People who used a middle initial were considered better
credit risks than those who didn’t. After an analysis by Mr. Meyer, he says, the company also began scoring first-time customers based on whether their phones were connected and their phone numbers legitimate. (Those whose phones did not work were considered at high risk of defaulting on payments.)

Using these different scoring techniques, Mr. Meyer says, Fingerhut could efficiently tailor its catalogs and offers to different customers; decide whether to approve or decline certain product orders; or choose which customer debts to collect on or write off.

“Without Fingerhut,” Mr. Meyer says, “I would never be in this business.” (Fingerhut is now an online and catalog retailer.)

In the 1990s, Mr. Meyer decided to use his expertise in spotting patterns of fraud to start RiskWise, an analytics enterprise of his own. After selling it, and two other companies, to LexisNexis in 2000 for about $89 million, he founded another start-up: a predictive analytics company that would become eBureau.

EVERY business needs customers. But how do you find them, and how do you know they will be good ones? In 2006, Mr. Meyer began to answer that question by carving a niche for himself in a nascent online industry called “lead generation.”

Lead generators are companies that set up consumer-friendly Web sites with the goal of funneling potential customers to businesses ranging from financial institutions to wedding photographers. It is a multibillion-dollar industry in the United States, says Jay Weintraub, chief executive of LeadsCon, a conference for Web sites that specializes in online customer acquisition.

Lead-generation sites like Bankrate.com, for example, offer rate calculators and other tools that prompt people to fill out forms with their names and contact information. The sites then transmit those consumers’ information to mortgage brokers, credit card issuers, car insurers and the like, offering access to these prospective customers, or leads, in return for a finder’s fee. The price varies. Lead generators may charge $8 for an insurance prospect; $35 for a finance lead; or $75 for a mortgage prospect, Mr. Meyer says.
But, he says, some companies were buying more than 100,000 leads a month without being able to distinguish one from another. They couldn’t sort potentially profitable customers from window-shoppers and fakes.

“Are people who are filling out the forms telling the truth? Because Yogi Bear and Fred Flintstone don’t buy a lot of stuff,” Mr. Meyer says. “Companies needed to figure out whether these leads were quality or not.”

Big national and international brands, Mr. Meyer knew, already employed data analytics to rate consumers. To distinguish his firm, he developed eBureau to offer customized scoring systems to midsize companies.

Here’s how eScores work:

A client submits a data set containing names of tens of thousands of sales leads it has already bought, along with the names of leads who went on to become customers. EBureau then adds several thousand details — like age, income, occupation, property value, length of residence and retail history — from its databases to each customer profile. From those raw data points, the system extrapolates up to 50,000 additional variables per person. Then it scours all that data for the rare common factors among the existing customer base. The resulting algorithm scores prospective customers based on their resemblance to previous customers.

EScores might range from 0 to 99, with 99 indicating a consumer who is a likely return on investment and 0 indicating an unprofitable one. But in some industries, “knowing the bottom is more important than knowing the top,” Mr. Meyer says. In online education, for instance, scores help schools winnow prospective students who are not worth the investment of expensive course catalogs or attentive follow-up calls — like people who use fake names or adopt the identities of relatives.

“If we can find 25 percent who have zero chance of enrolling, we can say ‘don’t waste your money on them,’ ” he says.
EBureau charges clients 3 to 75 cents a score, depending on the industry and the volume of leads.

Such scores increase the accuracy and speed with which companies can identify potential customers, says Mr. Weintraub of the LeadsCon conference.

“Scores tell you ‘this person might actually qualify, so let’s focus on them,’ ” he says. “This way you are not focusing on people who really can’t qualify.”

MOST people never see their value scores. But some services openly discuss how their measurements work. A case study on the eBureau site, for example, describes how the company ranked prospective customers for a national prepaid debit card issuer, assigning each a score of 0 to 998. People who scored above 950 were considered likely to become highly profitable customers, generating revenue over six months of an estimated $213 per card. Those who scored less than 550 were predicted to be unprofitable clients, with estimated revenue of $74 or less. With e-Bureau’s system, the card issuer could identify and court the high scorers while avoiding low scorers.

TargusInfo, a subsidiary of Neustar that is an eBureau competitor, is even more explicit about how a multinational credit card issuer used its scores.

According to a case study on its site, TargusInfo instantly scores prospective customers who call the card company’s call centers, selecting the kind of card to offer even before an agent picks up the phone. The scores also alert agents to high-value prospects, people “who are more likely to apply, be approved, request supplemental cards or spend more in their first year,” the case study says. While high-value callers are immediately routed to dedicated agents, it says, “less-qualified callers no longer waste the valuable time of the card issuer’s dedicated agents and are routed to an outsourced overflow call center.”

Becky Burr, chief privacy officer of Neustar, sees TargusInfo’s scoring system as a modern incarnation of marketing services to help companies find and communicate with their audiences.
“They want to allocate their marketing money efficiently, and consumers want messages that are relevant,” she says. The scores, she adds, should be seen as predictions about groups of consumers, not judgments on individuals.

For companies, this kind of scoring clearly increases the speed and reduces the cost of acquiring customers. But consumers are paying a heavy price for that increased corporate efficiency, public interests advocates say.

The digital scores create a two-tiered system that invisibly prioritizes some online users for credit and insurance offers while denying the same opportunities to others, says Mr. Mierzwinski of the Public Interest Research Group. The decades-old federal law that protects consumers from unfair credit practices, he says, has not kept pace with online innovation.

The Fair Credit Reporting Act requires that consumer reporting agencies, the companies that compile credit data, show people their credit reports and allow them to correct errors. Companies that use the reports must notify consumers if they take adverse action based on information in those reports. But digital marketers, Mr. Mierzwinski says, are able to work around the rules by using alternative financial data to calculate consumer scores. In an article scheduled to be published next spring in the Suffolk University Law Review, Mr. Mierzwinski and a co-author argue that new digital techniques like scoring let sales agents rapidly convert online prospects to customers, blurring the line between marketing and actual credit offers.

“The relationship between marketing and making a distinct offer of credit to a consumer is becoming blurred given contemporary digital marketing practices,” Mr. Mierzwinski and his co-author, Jeffrey Chester of the Center for Digital Democracy, write in the article. Federal regulators, they add, “should ensure consumers know whether and how they have been secretly scored or rated by the digital financial marketers, especially those labeled as less profitable or desirable.”

Mr. Meyer and other eBureau executives disagree, saying the concerns are misplaced.
EBureau, Mr. Meyer says, went to great lengths to build a system with both regulatory requirements and consumer privacy in mind. The company, he says, has put firewalls in place to separate databases containing federally regulated data, like credit or debt information used for purposes like risk management, from databases about consumers used to generate scores for marketing purposes.

He adds that eBureau’s clients use the scores only to narrow their field of prospective customers — not for the purposes of approving people for credit, loans or insurance. Moreover, he says, the company does not sell consumer data to others, nor does it retain the scores it transmits to clients.

“We are an evaluator,” Mr. Meyer says. “We are trying to stay away from being intrusive to the consumer.”

At a LeadsCon conference in Midtown Manhattan last month, eBureau was among those making its sales pitch. Its exhibition booth depicted a multiethnic group of fictional consumers and their hypothetical scores.

Score boxes superimposed over a young African-American male read variously: “eScore: 811, high lifetime value potential” and “eScore: 524, underbanked, but safe credit risk.” Another caption floating over the crowd read: “eScore: 906, route to best call center agent NOW!”

It’s just another sign of the rise of what might be called the Scored Society. Google ranks our search results by our location and search history. Facebook scores us based on our online activities. Klout scores us by how many followers we have on Twitter, among other things.

And now e-scores rank our potential value to companies.

But the spread of consumer rankings raises deep questions of fairness, says Frank Pasquale, a professor at Seton Hall University School of Law, who is writing a book about scoring technologies. The scores may help companies, he says. But over time, they may send some consumers into a downward spiral, locking them into a world of digital disadvantage.
“I’m troubled by the idea that some people will essentially be seeing ads for subprime loans, vocational schools and payday loans,” Professor Pasquale says, “while others might be seeing ads for regular banks and colleges, and not know why.”

This is the second in a series about the business of consumer data.

A version of this article appears in print on August 19, 2012, on page BU1 of the New York edition with the headline: Shoppers, Meet Your Scorekeeper.
YOU can be sold in seconds.

No, wait: make that milliseconds.

The odds are that access to you — or at least the online you — is being bought and sold in less than the blink of an eye. On the Web, powerful algorithms are sizing you up, based on myriad data points: what you Google, the sites you visit, the ads you click. Then, in real time, the chance to show you an ad is auctioned to the highest bidder.

Not that you’d know it. These days in the hyperkinetic world of digital advertising, all of this happens automatically, and imperceptibly, to most consumers.

Ever wonder why that same ad for a car or a couch keeps popping up on your screen? Nearly always, the answer is real-time bidding, an electronic trading system that sells ad space on the Web pages people visit at the very moment they are visiting them. Think of these systems as a sort of Nasdaq stock market, only trading in audiences for online ads. Millions of bids flood in every second. And those bids — essentially what your eyeballs are worth to advertisers — could determine whether you see an ad for, say, a new Lexus or a used Ford, for sneakers or a popcorn maker.

One big player in this space is the Rubicon Project. Never heard of it? Consider
Rubicon, based in Los Angeles, has actually eclipsed Google in one crucial area — the percentage of Internet users in the United States reached by display ads sold through its platform, according to comScore, a digital analytics company.

Rubicon is among a handful of technology companies that have quietly developed automated ad sales systems for Web site operators. The bidders are marketers seeking to identify their best prospects and pitch them before they move to the next Web page. It is a form of high-frequency trading — that souped-up business of algorithm-loving Wall Streeters. But in this case, the prize is the attention of ordinary people. And it all depends on data-mining to instantly evaluate the audiences available to see those online display ads, the ones that appear on Web sites next to or around content.

In industry parlance, each digital ad space is an impression. The value of an impression depends on several factors, like the size of the ad, the type of person who is available to see it and that person’s location.

“The first impression seen by a high-value person on the opening page of a major newspaper first thing in the morning has a different value than a user from China who is 12 and has been on the Web all day long playing games,” says Frank Addante, the founder and chief executive of Rubicon.

Yet for most of us, real-time bidding is invisible. About 97 percent of American Internet users interact with Rubicon’s system every month, Mr. Addante says, and most of them aren’t aware of it.

That worries some federal regulators and consumer advocates, who say that such electronic trading systems could unfairly stratify consumers, covertly offering better pricing to certain people while relegating others to inferior treatment. A computer-generated class system is one risk, they say, of an ad-driven Internet powered by surveillance.

“As you profile more and more people, you’ll start to segregate people into ‘the people you can get money out of’ and ‘the people you can’t get money out of,’ ” says Dan Auerbach, a staff technologist at the Electronic Frontier Foundation, a digital
civil rights group in San Francisco, who formerly worked in digital ad data-mining. “That is one of the dangers we should be worried about.”

Of course, ad agencies and brands can tailor ads to Web users without real-time bidding. They can also buy ads without aiming them at narrow audience groups. But for marketers, the marriage of ad- and audience-buying is one of the benefits of real-time bidding.

Not so long ago, they simply bought ad spaces based on a site’s general demographics and then showed every visitor the same ad, a practice called “spray and pray.” Now marketers can aim just at their ideal customers — like football fans who earn more than $100,000 a year, or mothers in Denver in the market for an S.U.V. — showing them tailored ads at the exact moment they are available on a specific Web page.

“We are not buying content as a proxy for audience,” says Paul Alfieri, the vice president for marketing at Turn, a data management company and automated buy-side platform for marketers based in Redwood City, Calif. “We are just buying who the audience is.”

Still, for many consumer advocates, real-time bidding resembles nothing so much as a cattle auction.

“Online consumers are being bought and sold like chattel,” says Jeffrey Chester, the executive director of the Center for Digital Democracy, a consumer group in Washington that has filed a complaint about real-time bidding with the Federal Trade Commission. “It’s dehumanizing.”

FRANK ADDANTE is 36 years old and given to wearing black shirts with a white Rubicon logo on the front. Rubicon is the fifth company he has started or helped to found.

In 1996, in his dorm room at the Illinois Institute of Technology, he developed and introduced a search engine. He later helped found L90, a digital ad technology company that went public and was later acquired by DoubleClick. His fourth
enterprise, StrongMail Systems, provides e-mail delivery infrastructure to large companies.

While working in ad technology, Mr. Addante says, he became puzzled by the manual ad sales processes that many Web sites were using. Just a few years ago, he recalled, many sites still executed their online ad deals through the cumbersome back-and-forth of meetings, phone calls, e-mails and even faxes. The fragmented market made it hard for ad agencies and brands.

“That market was very inefficient,” Mr. Addante said in an interview in Rubicon’s Manhattan office, “much like the early days of manual stock trading.”

Of course, other major industries already had automated sales systems. Concert arenas sold seats through Ticketmaster. Airlines sold tickets through a system called Sabre. Hotels offered rooms through Expedia.

So, in 2007, Mr. Addante and three other executives with whom he worked at L90, started Rubicon with the aim of creating an automated marketplace for Web sites to sell their ad inventory. Years earlier, Google invented a similar automated system for search ads.

“Google was the first to automate the buying and selling of search ads,” Mr. Addante says. “We thought, ‘why couldn’t we do this with display ads, mobile and video?’ ”

Although real-time bidding accounts for a small portion of online ad sales, it is growing fast. This year in the United States, advertisers are expected to spend about $2 billion on display ads bought through electronic auction-based exchanges, versus about $733 million in 2010, according to a recent report from Forrester Research. By 2017, the report estimated, that market is likely to reach $8.3 billion.

Rubicon’s customers now include ABC, eBay, CareerBuilder, Glam Media, Time Inc., the Drudge Report and Zynga. Its competitors include major players like PubMatic and Google’s DoubleClick ad exchange.
But Rubicon is not just a sales platform for Web site operators. It’s an analytics system that uses consumer data to help sites figure out how much their visitors are worth to advertisers.

Most sites, Mr. Addante explains, compile data about their own visitors through member registration or by placing bits of computer code called cookies on people’s browsers to collect information about their online activities. To those first-party profiles, Rubicon typically adds details from third-party data aggregators, like BlueKai or eXelate, such as users’ sex and age, interests, estimated income range and past purchases. Finally, Rubicon applies its own analytics to estimate the fair market value of site visitors and the ad spaces they are available to see.

The whole process typically takes less than 30 milliseconds.

“All these calculations have to happen before the Web page loads,” Mr. Addante says. “In our system, inventory is perishable.”

The competition for pricing accuracy has made companies involved in real-time bidding among the Internet’s most aggressive consumer trackers. Among the trackers setting the most cookies on the top 1,000 Web sites in the United States, for example, BlueKai was first, with 2,562 cookies, while Rubicon came in second, with 2,470, according to research conducted last month by the Berkeley Center for Law and Technology.

Consumer advocates say real-time bidding companies are acquiring and commoditizing all of that consumer data with little benefit to consumers themselves — and much digital snooping.

Mr. Addante and other industry executives disagree, saying consumers benefit by receiving ads and offers specifically relevant to them. Their systems do not invade privacy, they say, because they use numerical customer codes — not real names or other identifying details — to collect “anonymous” information about people’s online activities.

For many consumers, however, that Web and search history may seem
personal, especially if they visit financial or health sites. Some computer scientists argue that the customer codes assigned to online users are unique ID’s, allowing companies to compile portraits about millions of people — without needing to know their names. Moreover, a few researchers have reported that many sites leak personal information, like names and addresses, to third-party trackers operating on their sites.

That means that rather than being anonymous, those customer code numbers are pseudonymous at best, some computer researchers say.

“It’s like a Social Security number, a number that businesses can use to recognize you on your future visits,” says Rob van Eijk, a computer science researcher at Leiden University in the Netherlands, where he is studying real-time bidding. Yet, he adds, consumers generally remain in the dark as to how automated trading systems rank and shunt them. “Envision a Kafkaesque future,” he said, “where decisions are being made about you and you don’t know what the criteria are based on.”

TICK. Tick. Tick. Tick.

The horizontal ticker at the bottom of Turn’s buy-side trading dashboard registers the groups of users available now to see ads — and lists the bids that Turn’s system recommends for access to them.

The ad spaces, or impressions, sell in lots of 1,000. The price depends on variables like the size and type of ad space, the type of user, and whether the user is in an urban or rural location.

One moment, Turn’s system recommends that an insurance customer bid up to $35.70 per lot being sold by Facebook Exchange, a Facebook service that auctions ad space on the social networking site, and $1.35 per lot being offered by AppNexus, another sell-side platform. That means Turn has identified Facebook’s lots as “premium inventory,” says Mr. Alfieri, Turn’s vice president for marketing, while AppNexus is selling ads on sites where little is known about the users available to see them.
Real-time dashboards like Turn’s, he says, have modernized the online ad trade in the same way that Bloomberg terminals revolutionized Wall Street trading. Ad agencies and brands can now check the intraday prices for various impressions. Many ad agencies have even created in-house “trading desks” to monitor and adjust their bids.

But Turn’s dashboard is more than a real-time ticker. It’s an analytics system that enables clients like insurers or car companies to identify common details among their best customer segments and then bid to show ads to people who resemble those best customers. The machine learning process gets better at pinpointing ideal audiences over the course of an ad campaign.

For example, Turn recently ran an ad campaign for a sneaker company that initially chose to buy a wide variety of impressions nationwide. But as Turn’s system analyzed the early sets of results, it began to separate audiences into the kinds of people who clicked on those sneaker ads, or later searched for the shoes on their own, and those who did not. Identifying common details among those people required the system to comb through its databank of nearly a billion user profiles for each transaction.

(Like Rubicon, Turn uses consumer data from third-party data aggregators for its analyses, Mr. Alfieri said, adding that the company has hired outside software services to strip names and other details from the profiles before Turn receives them).

The results of the sneaker campaign were surprising, says Bill Demas, the chief executive of Turn.

“It turned out that Republicans in certain districts of Texas basically did not exercise. We were able to adjust the campaign to try to aim more at Democrats,” Mr. Demas says. Without analyzing those user profiles, he says, “who would think that party affiliation would be an influence in advertising campaigns?”

In some ways, the consumer segmentation process is not as newfangled as it may seem. For decades in the bricks-and-mortar world, direct marketers have
hired third-party data resellers to help them decide which customers should get catalogs or special offers in the mail. Real-time bidding is just a faster, smarter, more automated process for brands to find prospects likely to be the best fit for their products, says Joe Zawadzki, C.E.O. of MediaMath, a buy-side trading platform and data management company in Manhattan.

“How much is a rich person worth? To Mercedes, a lot. To a used Pinto dealer, not a lot,” he says. “It’s a different set of impressions for every marketer. That’s where the magic happens.”

But privacy advocates argue that real-time bidding is more problematic than direct mail because it often involves dozens of business-to-business companies — whose names most consumers have never heard of — collecting information and making instant decisions about them. The concern, advocates say, is that the very same automated bidding system that can distinguish coffee drinkers from, say, tea drinkers, and set different prices to show them ads, is also capable of distinguishing shopaholics or people in debt and potentially auctioning them to high-interest payday lenders.

“The reality looks like ‘we know a person is a sucker and they spend a lot of money on dumb things,’ ” says Mr. Auerbach of the Electronic Frontier Foundation. “Advertisers will spend more money to target them, and they aren’t savvy enough to know what is happening to them.”

As real-time bidding gains traction, the consumer data-mining that fuels it is escalating. Yet that surge in surveillance may present a serious risk for online businesses.

The volume of data collection on the Web has surged 400 percent, from an average of 10 collections a page in 2011 to 50 a page this year, according to a study published last June by Krux, a company that helps businesses protect and monetize their consumer data. The report attributed the explosive growth to the ad industry’s shift to real-time bidding.

Krux also warned Web site operators about what it called “rogue data
collection.” When publishers allow third parties, like real-time bidding platforms or information resellers, to collect data on their site, the report said, those partners often bring in other data miners whose practices the sites themselves cannot control. Those middlemen may use a site’s proprietary data to help competitors, the report said.

“Publishers who leak data leak revenue,” the report warned. “They face threats from middlemen who steal data and use it to create directly competitive audience-based offerings.”

Those threats may increase as real-time bidding moves more aggressively into mobile sites and apps, entities that may collect valuable information about users’ real-time locations and geographic patterns.

In May, Rubicon acquired Mobsmith, a start-up specializing in mobile ad technology. A few months later, the company announced that it was integrating real-time bidding for mobile ads into its system. Mr. Addante says he expects the industry to adopt real-time bidding for mobile ads faster than it had for desktop display ads. He also predicts that consumers will find tailored mobile ads for, say, a cafe or taxi in their vicinity, more pertinent than many Web ads tailored to them.

“I think mobile ads become more of an information provider than what is happening in display advertising where it has become a nuisance,” he says.

Yet the prospect of ubiquitous real-time bidding — online, on mobile devices and eventually on Web-enabled televisions — also hastens our transition to a totally traceable society. What we read and how we spend our spare time used to be private. Now those activities are becoming windows through which marketers scrutinize, appraise and vie to influence us for a price. Soon there may be no personal spaces left for our private thoughts.

“Real-time bidding creates the possibility for companies to tag you wherever you are going, without you knowing or having the ability to influence it,” says Mr. van Eijk, the computer scientist. “It is becoming a huge imbalance for the ordinary user because, in the end, the ordinary user is the product.”
Joseph J. Atick cased the floor of the Ronald Reagan Building and International Trade Center in Washington as if he owned the place. In a way, he did. He was one of the organizers of the event, a conference and trade show for the biometrics security industry. Perhaps more to the point, a number of the wares on display, like an airport face-scanning checkpoint, could trace their lineage to his work.

A physicist, Dr. Atick is one of the pioneer entrepreneurs of modern face recognition. Having helped advance the fundamental face-matching technology in the 1990s, he went into business and promoted the systems to government agencies looking to identify criminals or prevent identity fraud. “We saved lives,” he said during the conference in mid-March. “We have solved crimes.”

Thanks in part to his boosterism, the global business of biometrics — using people’s unique physiological characteristics, like their fingerprint ridges and facial features, to learn or confirm their identity — is booming. It generated an estimated $7.2 billion in 2012, according to reports by Frost & Sullivan.

Making his rounds at the trade show, Dr. Atick, a short, trim man with an indeterminate Mediterranean accent, warmly greeted industry representatives at their exhibition booths. Once he was safely out of earshot, however, he worried aloud about what he was seeing. What were those companies’ policies for retaining and reusing consumers’ facial data? Could they identify individuals without their
explicit consent? Were they running face-matching queries for government agencies on the side?

Now an industry consultant, Dr. Atick finds himself in a delicate position. While promoting and profiting from an industry that he helped foster, he also feels compelled to caution against its unfettered proliferation. He isn’t so much concerned about government agencies that use face recognition openly for specific purposes — for example, the many state motor vehicle departments that scan drivers’ faces as a way to prevent license duplications and fraud. Rather, what troubles him is the potential exploitation of face recognition to identify ordinary and unwitting citizens as they go about their lives in public. Online, we are all tracked. But to Dr. Atick, the street remains a haven, and he frets that he may have abetted a technology that could upend the social order.

Face-matching today could enable mass surveillance, “basically robbing everyone of their anonymity,” he says, and inhibit people’s normal behavior outside their homes. Pointing to the intelligence documents made public by Edward J. Snowden, he adds that once companies amass consumers’ facial data, government agencies might obtain access to it, too.

To many in the biometrics industry, Dr. Atick’s warning seems Cassandra-like. Face recognition to them is no different from a car, a neutral technology whose advantages far outweigh the risks. The conveniences of biometrics seem self-evident: Your unique code automatically accompanies you everywhere. They envision a world where, instead of having to rely on losable ID cards or on a jumble of easily forgettable — not to mention hackable — passwords, you could unlock your smartphone or gain entry to banks, apartment complexes, parking garages and health clubs just by showing your face.

Dr. Atick sees convenience in these kinds of uses as well. But he provides a cautionary counterexample to make his case. Just a few months back, he heard about NameTag, an app that, according to its news release, was available in an early form to people trying out Google Glass. Users had only to glance at a stranger and NameTag would instantly return a match complete with that stranger’s name,
occupation and public Facebook profile information. “We are basically allowing our fellow citizens to surveil us,” Dr. Atick told me on the trade-show floor.

(His sentiments were shared by Senator Al Franken, Democrat of Minnesota and chairman of the Senate subcommittee on privacy, technology and the law. Concerned that NameTag might facilitate stalking, Mr. Franken requested that its public introduction be delayed; in late April, the app’s developer said he would comply with the request. Google has said that it will not approve facial recognition apps on Google Glass.)

Dr. Atick is just as bothered by what could be brewing quietly in larger companies. Over the past few years, several tech giants have acquired face-recognition start-up businesses. In 2011, Google bought Pittsburgh Pattern Recognition, a computer vision business developed by researchers at Carnegie Mellon University. In 2012, Facebook bought Face.com, an Israeli start-up.

Google and Facebook both declined to comment for this article about their plans for the technology.

Dr. Atick says the technology he helped cultivate requires some special safeguards. Unlike fingerprinting or other biometric techniques, face recognition can be used at a distance, without people’s awareness; it could then link their faces and identities to the many pictures they have put online. But in the United States, no specific federal law governs face recognition. A division of the Commerce Department is organizing a meeting of industry representatives and consumer advocates on Tuesday to start hammering out a voluntary code of conduct for the technology’s commercial use.

Dr. Atick has been working behind the scenes to influence the outcome. He is part of a tradition of scientists who have come to feel responsible for what their work has wrought. “I think that the industry has to own up,” he asserts. “If we do not step up to the plate and accept responsibility, there could be unexpected apps and consequences.”

‘Not an Innocent Machine’
A few uses of face recognition are already commonplace. It’s what allows Facebook and Google Plus to automatically suggest name tags for members or their friends in photographs.

And more applications could be in the works. Google has applied for a patent on a method to identify faces in videos and on one to allow people to log on to devices by winking or making other facial expressions. Facebook researchers recently reported how the company had developed a powerful pattern-recognition system, called DeepFace, which had achieved near-human accuracy in identifying people’s faces.

But real-time, automated face recognition is a relatively recent phenomenon and, at least for now, a niche technology. In the early 1990s, several academic researchers, including Dr. Atick, hit upon the idea of programming computers to identify a face’s most distinguishing features; the software then used those local points to recognize that face when it reappeared in other images.

To work, the technology needs a large data set, called an image gallery, containing the photographs or video stills of faces already identified by name. Software automatically converts the topography of each face in the gallery into a unique mathematical code, called a faceprint. Once people are faceprinted, they may be identified in existing or subsequent photographs or as they walk in front of a video camera.

The technology is already in use in law enforcement and casinos. In New York, Pennsylvania and California, police departments with face-recognition systems can input the image of a robbery suspect taken from a surveillance video in a bank, for instance, and compare the suspect’s faceprint against their image gallery of convicted criminals, looking for a match. And some casinos faceprint visitors, seeking to identify repeat big-spending customers for special treatment. In Japan, a few grocery stores use face-matching to classify some shoppers as shoplifters or even “complainers” and blacklist them.

Whether society embraces face recognition on a larger scale will ultimately
depend on how legislators, companies and consumers resolve the argument about its singularity. Is faceprinting as innocuous as photography, an activity that people may freely perform? Or is a faceprint a unique indicator, like a fingerprint or a DNA sequence, that should require a person’s active consent before it can be collected, matched, shared or sold?

Dr. Atick is firmly in the second camp.

His upbringing influenced both his interest in identity authentication and his awareness of the power conferred on those who control it. He was born in Jerusalem in 1964 to Christian parents of Greek and French descent. Conflict based on ethnic and religious identity was the backdrop of his childhood. He was an outsider, neither Jewish nor Muslim, and remembers often having to show an identity booklet listing his name, address and religion.

“As a 5- or 6-year old boy, seeing identity as a foundation for trust, I think it marked me,” Dr. Atick says. To this day, he doesn’t feel comfortable leaving his New York apartment without his driver’s license or passport.

After a childhood accident damaged his eyesight, he became interested in the mechanics of human vision. Eventually, he dropped out of high school to write a physics textbook. His family moved to Miami, and he decided to skip college. It did not prove a setback; at 17, he was accepted to a doctoral program in physics at Stanford.

Still interested in how the brain processes visual information, he started a computational neuroscience lab at Rockefeller University in Manhattan, where he and two colleagues began programming computers to recognize faces. To test the accuracy of their algorithms, they acquired the most powerful computer they could find, a Silicon Graphics desktop, for their lab and mounted a video camera on it. They added a speech synthesizer so the device could read certain phrases aloud.

As Dr. Atick tells it, he concluded that the system worked after he walked into the lab one day and the computer called out his name, along with those of colleagues in the room. “We were just milling about and you heard this metallic
voice saying: ‘I see Joseph. I see Norman. I see Paul,’ ” Dr. Atick recounts. Until then, most face recognition had involved analyzing static images, he says, not identifying a face amid a group of live people. “We had made a breakthrough.”

The researchers left academia to start their own face-recognition company, called Visionics, in 1994. Dr. Atick says he hadn’t initially considered the ramifications of their product, named FaceIt. But when intelligence agencies began making inquiries, he says, it “started dawning on me that this was not an innocent machine.”

He helped start an international biometrics trade group, and it came up with guidelines like requiring notices in places where face recognition was in use. But even in a nascent industry composed of a few companies, he had little control.

In 2001, his worst-case scenario materialized. A competitor supplied the Tampa police with a face-recognition system; officers covertly deployed it on fans attending Super Bowl XXXV. The police scanned tens of thousands of fans without their awareness, identifying a handful of petty criminals, but no one was detained.

Journalists coined it the “Snooper Bowl.” Public outrage and congressional criticism ensued, raising issues about the potential intrusiveness and fallibility of face recognition that have yet to be resolved.

Dr. Atick says he thought this fiasco had doomed the industry: “I had to explain to the media this was not responsible use.”

Then, a few months later, came the Sept. 11 terrorist attacks. Dr. Atick immediately went to Washington to promote biometrics as a new method of counterterrorism. He testified before congressional committees and made the rounds on nightly news programs where he argued that terrorism might be prevented if airports, motor vehicle departments, law enforcement and immigration agencies used face recognition to authenticate people’s identities.

“Terror is not faceless,” he said in one segment on ABC’s “World News Tonight.” “Terror has measurable identity, has a face that can be detected through
technology that’s available today.”

It was an optimistic spin, given that the technology at that early stage did not work well in uncontrolled environments.

Still, Dr. Atick prospered. He merged his original business with other biometrics enterprises, eventually forming a company called L-1 Identity Solutions. In 2011, Safran, a military contractor in France, bought the bulk of that company for about $1.5 billion, including debt.

Dr. Atick had waited 17 years for a cash payout from his endeavors; his take amounted to tens of millions of dollars.

In fact, some experts view his contribution to the advancement of face recognition as not so much in research but in recognizing its business potential and capitalizing on it.

“He actually was one of the early commercializers of face-recognition algorithms,” says P. Jonathon Phillips, an electronics engineer at the National Institute of Standards and Technology, which evaluates the accuracy of commercial face-recognition engines.

Ovals, Squares and Matches

At Knickerbocker Village, a 1,600-unit red-brick apartment complex in Lower Manhattan where Julius and Ethel Rosenberg once lived, the entryways click open as residents walk toward the doors. It is one of the first properties in New York City to install a biometrics system that uses both face and motion recognition, and it is a showcase for FST Biometrics, the Israeli security firm that designed the program.

“This development will make obsolete keys, cards and codes — because your identity is the key,” says Aharon Zeevi Farkash, the chief executive of FST. “Your face, your behavior, your biometrics are the key.”

On a recent visit to New York, Mr. Farkash offered to demonstrate how it worked. We met at the Knickerbocker security office on the ground floor. There, he
posed before a webcam, enabling the system to faceprint and enroll him. To test it, he walked outside into the courtyard and approached one of the apartment complex entrances. He pulled open an outer glass door, heading directly toward a camera embedded in the wall near an inner door.

Back in the security office, a monitor broadcast video of the process.

First, a yellow oval encircled Mr. Farkash’s face in the video, indicating that the system had detected a human head. Then a green square materialized around his head. The system had found a match. A message popped up on the screen: “Recognized, Farkash Aharon. Confidence: 99.7 percent.”

On his third approach, the system pegged him even sooner — while he was opening the outer door.

Mr. Farkash says he believes that systems like these, which are designed to identify people in motion, will soon make obsolete the cumbersome, time-consuming security process at most airports.

“The market needs convenient security,” he told me; the company’s system is now being tested at one airport.

Mr. Farkash served in the Israeli army for nearly 40 years, eventually as chief of military intelligence. Now a major general in the army reserves, he says he became interested in biometrics because of two global trends: the growth of densely populated megacities and the attraction that dense populations hold for terrorists.

In essence, he started FST Biometrics because he wanted to improve urban security. Although the company has residential, corporate and government clients, Mr. Farkash’s larger motive is to convince average citizens that face identification is in their best interest. He hopes that people will agree to have their faces recognized while banking, attending school, having medical treatments and so on.

If all the “the good guys” were to volunteer to be faceprinted, he theorizes, “the
bad guys” would stand out as obvious outliers. Mass public surveillance, Mr. Farkash argues, should make us all safer.

Safer or not, it could have chilling consequences for human behavior.

A private high school in Los Angeles also has an FST system. The school uses the technology to recognize students when they arrive — a security measure intended to keep out unwanted interlopers. But it also serves to keep the students in line.

“If a girl will come to school at 8:05, the door will not open and she will be registered as late,” Mr. Farkash explained. “So you can use the system not only for security but for education, for better discipline.”

**Faceprints and Civil Liberties**

In February, Dr. Atick was invited to speak at a public meeting on face recognition convened by the National Telecommunications and Information Administration. It was part of an agency effort to corral industry executives and consumer advocates into devising a code for the technology’s commercial use.

But some tech industry representatives in attendance were reluctant to describe their plans or make public commitments to limit face recognition. Dr. Atick, who was serving on a panel, seemed to take their silence as an affront to his sense of industry accountability.

“Where is Google? Where is Facebook?” he loudly asked the audience at one point.

“Here,” one voice in the auditorium volunteered. That was about the only public contribution from the two companies that day.

The agency meetings on face recognition are continuing. In a statement, Matt Kallman, a Google spokesman, said the company was “participating in discussions to advance our view that the industry should make sure technology is in line with people’s expectations.”
A Facebook spokeswoman, Jodi Seth, said in a statement that the company was participating in the process. “Multi-stakeholder dialogues like this are critical to promoting people’s privacy,” she said, “but until a code of conduct exists, we can’t say whether we will sign it.”

The fundamental concern about faceprinting is the possibility that it would be used to covertly identify a live person by name — and then serve as the link that would connect them, without their awareness or permission, to intimate details available online, like their home addresses, dating preferences, employment histories and religious beliefs. It’s not a hypothetical risk. In 2011, researchers at Carnegie Mellon reported in a study that they had used a face-recognition app to identify some students on campus by name, linking them to their public Facebook profiles and, in some cases, to their Social Security numbers.

As with many emerging technologies, the arguments tend to coalesce around two predictable poles: those who think the technology needs rules and regulation to prevent violations of civil liberties and those who fear that regulation would stifle innovation. But face recognition stands out among such technologies: While people can disable smartphone geolocation and other tracking techniques, they can’t turn off their faces.

“Facial recognition involves the intersection of multiple research disciplines that have serious consequences for privacy, consumer protection and human rights,” wrote Jeffrey Chester, executive director of the nonprofit Center for Digital Democracy, in a recent blog post.

“Guidelines at this stage could stymie progress in a very promising market, and could kill investment,” Paul Schuepp, the chief executive of Animetrics, a company that supplies mobile face-recognition systems to the military, recently wrote on the company’s blog.

Dr. Atick takes a middle view.

To maintain the status quo around public anonymity, he says, companies should take a number of steps: They should post public notices where they use face
recognition; seek permission from a consumer before collecting a faceprint with a unique, repeatable identifier like a name or code number; and use faceprints only for the specific purpose for which they have received permission. Those steps, he says, would inhibit sites, stores, apps and appliances from covertly linking a person in the real world with their multiple online personas.

“Some people believe that I am maybe inhibiting the industry from growing. I disagree,” Dr. Atick told me. “I am helping industry make difficult choices, but the right choices.”

A version of this article appears in print on May 18, 2014, on page BU1 of the New York edition with the headline: Never Forgetting a Face.
AUTO INSURANCE

Lower Your Car Insurance Bill, at the Price of Some Privacy

AUG. 15, 2014

Your Money

By RON LIEBER

An increasing number of the nation’s auto insurance companies have a new proposition: Let them track every second of your driving in exchange for an annual discount that can reach into the hundreds of dollars if you behave yourself on the road.

In theory, everyone wins here. Progressive, Allstate and State Farm — among the most aggressive of the larger companies that are pursuing this strategy — attract better drivers who crash less often. Customers who sign up for the optional programs can pay premiums based more on how they drive and less on their age, gender or credit history.

But usage-based insurance, as the program is known, generates vast amounts of data. While insurance companies are pledging to keep it to themselves for now, some experts believe that we’re only a few years away from companies’ contributing complete driver histories into a central industry database. Then, we’d all have driver scores like the numbers that FICO helps creditors calculate, which would follow us around whenever we shopped for a new auto insurance policy.
How quickly that day comes will depend on how many people allow insurance companies to ride shotgun in the near future, since they can’t create scores unless they can persuade us to share our driving data. To see how it felt, my wife and I let State Farm keep an eye on us this summer.

State Farm sent us a device that we plugged into a port under the steering wheel of our 2003 Toyota Highlander. That was all we had to do to begin; the machine wirelessly transmitted data about our movements to the company.

A few weeks later, we started getting feedback in the form of a report card that State Farm issues to customers participating in its Drive Safe and Save program. The company assesses drivers in five categories — acceleration, deceleration, turns, time of day and speed — with grades ranging from A to C. (The company didn’t want to hurt anyone’s feelings by flunking them.) The grades are then plugged into a formula that determines discounts.

For now, the company’s interest in a customer’s speed extends only to whether you’re driving more than 80 miles per hour, and if so, for how long. We did just a bit while in a 65 m.p.h. zone on the Massachusetts Turnpike and ended up with an A-minus grade in that category. Our lead foot on the accelerator led to our worst grade, a B-plus, in the acceleration category. The company has data showing correlations between higher claims and repeated instances of increasing speed more than 5 m.p.h. in less than a second. Our A-minus on deceleration meant that we didn’t slow down by more than 10 m.p.h. in less than a second too often, an indication that we weren’t slamming on the brakes much and were probably paying decent attention to the road.

Our A-minus on turns was a pleasant surprise given the number of curves we encountered while driving on vacation, but the device can measure the G forces exerted from each turn and we mostly passed muster there. Our only perfect grade was in the time-of-day category, as we didn’t drive during rush hour and we stay off the roads from midnight to 4 a.m. when the drunk and exhausted are out in force.

For our above-average efforts, State Farm said we would have qualified for a
22 percent annual discount on a policy with generous coverage limits in New Jersey if we drove about 10,000 miles a year, reflecting a $190 discount off an initial $870 premium.

Over all, participants in the program get an average of 10 to 15 percent off their premium, and everyone gets at least something for playing along. At Progressive’s Snapshot program, people who do qualify for the discount tend to save an average of 10 to 15 percent. Some other companies require you to keep the in-vehicle device for continuous monitoring (and possible price adjustments later) and may make you pay a fee for it plus some ancillary services; others ask you to send it back after six months but allow for a retest later upon request.

At the moment, State Farm and Progressive are not raising rates on people who sign up for monitoring and prove to be terrible drivers. Participation is voluntary, and Progressive, the early adopter in usage-based insurance, says that close to 15 percent of its customers are already enrolled.

Still, as more people sign up, the standard rate will start to feel like a penalty for those who decline to participate. And if all of the good drivers pile into the programs and qualify for lower prices, the companies may eventually raise rates on the holdouts. One bonus for parents who are on the fence: You can often use an insurer’s usage-based insurance or related tracking programs to monitor your teenager’s driving. And Safeco Insurance has an interesting twist, in which people who have gotten speeding tickets or been in accidents can use a monitoring device to requalify for the rate they had before the black mark went on their records.

Given all these incentives, why might someone hold out?

First, not every company offers a usage-based insurance policy. Our insurance company, USAA, does not, although it has started a pilot program to gather data. Geico has no program either, and a spokeswoman declined to comment on the reason. Progressive, State Farm, Allstate and others have policies or pilot programs, but people in certain states or who drive vehicles that are incompatible with the companies’ hardware may not be able to sign up or may not be able to
share as much driving data.

But privacy is the biggest concern. While the major players are not yet tracking exact latitude or longitude, they would like to, and Progressive is testing it. “A mile driven on a highway is safer than a mile on a city street with lots of intersections, but in today’s world we don’t know which road you’re on,” said Dave Pratt, general manager of usage-based insurance at Progressive. Some customers are already asking for the company to track them in this way.

The companies probably have little interest in who you’re visiting or patronizing on any given day, but divorce lawyers and others may one day subpoena the information if insurance companies store it. The data can work in drivers’ favor too, though; one Progressive customer used his driving data to prove that he did not kill his infant daughter, who died of asphyxiation at her home. The company can also pull the data if you think it might help you avoid fault when you’re making a claim; so far, it is not doing this unless customers ask it to, though it’s hard to imagine that insurance companies won’t eventually be grabbing for the information while examining future claims.

For those of us with no privacy concerns, it’s difficult to make a solid case against usage-based insurance. For me, it turned driving into a game that could yield real money through safer behavior. Progressive’s data already shows that people learn to brake more gently within weeks of signing up; unlike with State Farm, Progressive’s device beeps when you’re slowing down too fast. The companies are betting that by giving safer drivers better deals, they will retain them longer and make up for the discounts with fewer claims over time. Plus, the front-runners in the industry will undoubtedly attract good drivers from competitors that don’t offer the discounts, leaving the laggards with potentially higher costs from those who remain.

The one lingering worry is that possibility of a FICO-like driver score. The leading companies in usage-based insurance say they want nothing of the sort. After all, they have more data than their competitors, so why would they share it?
Unsurprisingly, the companies that could benefit from universal driver scores by helping insurers collect the data believe such a score is inevitable. “I don’t see how it doesn’t happen,” said David Lukens, director of vertical markets at LexisNexis Risk Solutions, which already helps auto insurers generate scores internally, ranging from 200 to 997. “There will be a tipping point where if most companies have this data, they’re going to weigh the costs and benefits of sharing it.”

While insurers currently promise to keep customer data to themselves, they could end that agreement starting on a certain date. In fact, it may be customers who ask them to do so when they inevitably go from feeling grateful for the discounts to feeling captive because no other company knows what a great driver they are. “People are going to want to say that the driving data is mine, and I want the ability to shop that around in the same way that they do with credit data,” said Brian Sullivan, editor of the Auto Insurance Report.

Which is fine, as long as the data is correct. It won’t be, because no system is perfect, though one hopes it will not be as error-strewn as credit reports are today. But that’s a concern for the future. For now, anyone with little to hide and a desire to drive better can help themselves to some free money while the insurance companies fight over the more careful drivers among us.

Twitter: @ronlieber

Make the most of your money. Every Monday get articles about retirement, saving for college, investing, new online financial services and much more. Sign up for the Your Money newsletter here.

A version of this article appears in print on August 16, 2014, on page B1 of the New York edition with the headline: Safety Spies.
How Companies Learn Your Secrets

By CHARLES DUHIGG  FEB. 16, 2012

Andrew Pole had just started working as a statistician for Target in 2002, when two colleagues from the marketing department stopped by his desk to ask an odd question: “If we wanted to figure out if a customer is pregnant, even if she didn’t want us to know, can you do that?”

Pole has a master’s degree in statistics and another in economics, and has been obsessed with the intersection of data and human behavior most of his life. His parents were teachers in North Dakota, and while other kids were going to 4-H, Pole was doing algebra and writing computer programs. “The stereotype of a math nerd is true,” he told me when I spoke with him last year. “I kind of like going out and evangelizing analytics.”

As the marketers explained to Pole — and as Pole later explained to me, back when we were still speaking and before Target told him to stop — new parents are a retailer’s holy grail. Most shoppers don’t buy everything they need at one store. Instead, they buy groceries at the grocery store and toys at the toy store, and they visit Target only when they need certain items they associate with Target — cleaning supplies, say, or new socks or a six-month supply of toilet paper. But Target sells everything from milk to stuffed animals to lawn furniture to electronics, so one of the company’s primary goals is convincing customers that the only store they need is Target. But it’s a tough message to get across, even with the most ingenious ad campaigns, because once consumers’ shopping habits are ingrained, it’s incredibly difficult to change them.
There are, however, some brief periods in a person’s life when old routines fall apart and buying habits are suddenly in flux. One of those moments — the moment, really — is right around the birth of a child, when parents are exhausted and overwhelmed and their shopping patterns and brand loyalties are up for grabs. But as Target’s marketers explained to Pole, timing is everything. Because birth records are usually public, the moment a couple have a new baby, they are almost instantaneously barraged with offers and incentives and advertisements from all sorts of companies. Which means that the key is to reach them earlier, before any other retailers know a baby is on the way. Specifically, the marketers said they wanted to send specially designed ads to women in their second trimester, which is when most expectant mothers begin buying all sorts of new things, like prenatal vitamins and maternity clothing. “Can you give us a list?” the marketers asked.

“We knew that if we could identify them in their second trimester, there’s a good chance we could capture them for years,” Pole told me. “As soon as we get them buying diapers from us, they’re going to start buying everything else too. If you’re rushing through the store, looking for bottles, and you pass orange juice, you’ll grab a carton. Oh, and there’s that new DVD I want. Soon, you’ll be buying cereal and paper towels from us, and keep coming back.”

The desire to collect information on customers is not new for Target or any other large retailer, of course. For decades, Target has collected vast amounts of data on every person who regularly walks into one of its stores. Whenever possible, Target assigns each shopper a unique code — known internally as the Guest ID number — that keeps tabs on everything they buy. “If you use a credit card or a coupon, or fill out a survey, or mail in a refund, or call the customer help line, or open an e-mail we’ve sent you or visit our Web site, we’ll record it and link it to your Guest ID,” Pole said. “We want to know everything we can.”

Also linked to your Guest ID is demographic information like your age, whether you are married and have kids, which part of town you live in, how long it takes you to drive to the store, your estimated salary, whether you’ve moved recently, what credit cards you carry in your wallet and what Web sites you visit. Target can buy data about your ethnicity, job history, the magazines you read, if
you’ve ever declared bankruptcy or got divorced, the year you bought (or lost) your house, where you went to college, what kinds of topics you talk about online, whether you prefer certain brands of coffee, paper towels, cereal or applesauce, your political leanings, reading habits, charitable giving and the number of cars you own. (In a statement, Target declined to identify what demographic information it collects or purchases.) All that information is meaningless, however, without someone to analyze and make sense of it. That’s where Andrew Pole and the dozens of other members of Target’s Guest Marketing Analytics department come in.

Almost every major retailer, from grocery chains to investment banks to the U.S. Postal Service, has a “predictive analytics” department devoted to understanding not just consumers’ shopping habits but also their personal habits, so as to more efficiently market to them. “But Target has always been one of the smartest at this,” says Eric Siegel, a consultant and the chairman of a conference called Predictive Analytics World. “We’re living through a golden age of behavioral research. It’s amazing how much we can figure out about how people think now.”

The reason Target can snoop on our shopping habits is that, over the past two decades, the science of habit formation has become a major field of research in neurology and psychology departments at hundreds of major medical centers and universities, as well as inside extremely well financed corporate labs. “It’s like an arms race to hire statisticians nowadays,” said Andreas Weigend, the former chief scientist at Amazon.com. “Mathematicians are suddenly sexy.” As the ability to analyze data has grown more and more fine-grained, the push to understand how daily habits influence our decisions has become one of the most exciting topics in clinical research, even though most of us are hardly aware those patterns exist. One study from Duke University estimated that habits, rather than conscious decision-making, shape 45 percent of the choices we make every day, and recent discoveries have begun to change everything from the way we think about dieting to how doctors conceive treatments for anxiety, depression and addictions.

This research is also transforming our understanding of how habits function across organizations and societies. A football coach named Tony Dungy propelled
one of the worst teams in the N.F.L. to the Super Bowl by focusing on how his players habitually reacted to on-field cues. Before he became Treasury secretary, Paul O’Neill overhauled a stumbling conglomerate, Alcoa, and turned it into a top performer in the Dow Jones by relentlessly attacking one habit — a specific approach to worker safety — which in turn caused a companywide transformation. The Obama campaign has hired a habit specialist as its “chief scientist” to figure out how to trigger new voting patterns among different constituencies.

Researchers have figured out how to stop people from habitually overeating and biting their nails. They can explain why some of us automatically go for a jog every morning and are more productive at work, while others oversleep and procrastinate. There is a calculus, it turns out, for mastering our subconscious urges. For companies like Target, the exhaustive rendering of our conscious and unconscious patterns into data sets and algorithms has revolutionized what they know about us and, therefore, how precisely they can sell.

Inside the **brain-and-cognitive-sciences** department of the [Massachusetts Institute of Technology](http://www.mit.edu) are what, to the casual observer, look like dollhouse versions of surgical theaters. There are rooms with tiny scalpels, small drills and miniature saws. Even the operating tables are petite, as if prepared for 7-year-old surgeons. Inside those shrunken O.R.’s, neurologists cut into the skulls of anesthetized rats, implanting tiny sensors that record the smallest changes in the activity of their brains.

An M.I.T. neuroscientist named Ann Graybiel told me that she and her colleagues began exploring habits more than a decade ago by putting their wired rats into a T-shaped maze with chocolate at one end. The maze was structured so that each animal was positioned behind a barrier that opened after a loud click. The first time a rat was placed in the maze, it would usually wander slowly up and down the center aisle after the barrier slid away, sniffing in corners and scratching at walls. It appeared to smell the chocolate but couldn’t figure out how to find it. There was no discernible pattern in the rat’s meanderings and no indication it was working hard to find the treat.
The probes in the rats’ heads, however, told a different story. While each animal wandered through the maze, its brain was working furiously. Every time a rat sniffed the air or scratched a wall, the neurosensors inside the animal’s head exploded with activity. As the scientists repeated the experiment, again and again, the rats eventually stopped sniffing corners and making wrong turns and began to zip through the maze with more and more speed. And within their brains, something unexpected occurred: as each rat learned how to complete the maze more quickly, its mental activity decreased. As the path became more and more automatic — as it became a habit — the rats started thinking less and less.

This process, in which the brain converts a sequence of actions into an automatic routine, is called “chunking.” There are dozens, if not hundreds, of behavioral chunks we rely on every day. Some are simple: you automatically put toothpaste on your toothbrush before sticking it in your mouth. Some, like making the kids’ lunch, are a little more complex. Still others are so complicated that it’s remarkable to realize that a habit could have emerged at all.

Take backing your car out of the driveway. When you first learned to drive, that act required a major dose of concentration, and for good reason: it involves peering into the rearview and side mirrors and checking for obstacles, putting your foot on the brake, moving the gearshift into reverse, removing your foot from the brake, estimating the distance between the garage and the street while keeping the wheels aligned, calculating how images in the mirrors translate into actual distances, all while applying differing amounts of pressure to the gas pedal and brake.

Now, you perform that series of actions every time you pull into the street without thinking very much. Your brain has chunked large parts of it. Left to its own devices, the brain will try to make almost any repeated behavior into a habit, because habits allow our minds to conserve effort. But conserving mental energy is tricky, because if our brains power down at the wrong moment, we might fail to notice something important, like a child riding her bike down the sidewalk or a speeding car coming down the street. So we’ve devised a clever system to determine when to let a habit take over. It’s something that happens whenever a
chunk of behavior starts or ends — and it helps to explain why habits are so difficult to change once they’re formed, despite our best intentions.

To understand this a little more clearly, consider again the chocolate-seeking rats. What Graybiel and her colleagues found was that, as the ability to navigate the maze became habitual, there were two spikes in the rats’ brain activity — once at the beginning of the maze, when the rat heard the click right before the barrier slid away, and once at the end, when the rat found the chocolate. Those spikes show when the rats’ brains were fully engaged, and the dip in neural activity between the spikes showed when the habit took over. From behind the partition, the rat wasn’t sure what waited on the other side, until it heard the click, which it had come to associate with the maze. Once it heard that sound, it knew to use the “maze habit,” and its brain activity decreased. Then at the end of the routine, when the reward appeared, the brain shook itself awake again and the chocolate signaled to the rat that this particular habit was worth remembering, and the neurological pathway was carved that much deeper.

The process within our brains that creates habits is a three-step loop. First, there is a cue, a trigger that tells your brain to go into automatic mode and which habit to use. Then there is the routine, which can be physical or mental or emotional. Finally, there is a reward, which helps your brain figure out if this particular loop is worth remembering for the future. Over time, this loop — cue, routine, reward; cue, routine, reward — becomes more and more automatic. The cue and reward become neurologically intertwined until a sense of craving emerges. What’s unique about cues and rewards, however, is how subtle they can be. Neurological studies like the ones in Graybiel’s lab have revealed that some cues span just milliseconds. And rewards can range from the obvious (like the sugar rush that a morning doughnut habit provides) to the infinitesimal (like the barely noticeable — but measurable — sense of relief the brain experiences after successfully navigating the driveway). Most cues and rewards, in fact, happen so quickly and are so slight that we are hardly aware of them at all. But our neural systems notice and use them to build automatic behaviors.

Habits aren’t destiny — they can be ignored, changed or replaced. But it’s also
true that once the loop is established and a habit emerges, your brain stops fully participating in decision-making. So unless you deliberately fight a habit — unless you find new cues and rewards — the old pattern will unfold automatically.

“We’ve done experiments where we trained rats to run down a maze until it was a habit, and then we extinguished the habit by changing the placement of the reward,” Graybiel told me. “Then one day, we’ll put the reward in the old place and put in the rat and, by golly, the old habit will re-emerge right away. Habits never really disappear.”

**Luckily, simply understanding** how habits work makes them easier to control. Take, for instance, a series of studies conducted a few years ago at Columbia University and the University of Alberta. Researchers wanted to understand how exercise habits emerge. In one project, 256 members of a health-insurance plan were invited to classes stressing the importance of exercise. Half the participants received an extra lesson on the theories of habit formation (the structure of the habit loop) and were asked to identify cues and rewards that might help them develop exercise routines.

The results were dramatic. Over the next four months, those participants who deliberately identified cues and rewards spent twice as much time exercising as their peers. Other studies have yielded similar results. According to another recent paper, if you want to start running in the morning, it’s essential that you choose a simple cue (like always putting on your sneakers before breakfast or leaving your running clothes next to your bed) and a clear reward (like a midday treat or even the sense of accomplishment that comes from ritually recording your miles in a log book). After a while, your brain will start anticipating that reward — craving the treat or the feeling of accomplishment — and there will be a measurable neurological impulse to lace up your jogging shoes each morning.

Our relationship to e-mail operates on the same principle. When a computer chimes or a smartphone vibrates with a new message, the brain starts anticipating the neurological “pleasure” (even if we don’t recognize it as such) that clicking on the e-mail and reading it provides. That expectation, if unsatisfied, can build until
you find yourself moved to distraction by the thought of an e-mail sitting there unread — even if you know, rationally, it’s most likely not important. On the other hand, once you remove the cue by disabling the buzzing of your phone or the chiming of your computer, the craving is never triggered, and you’ll find, over time, that you’re able to work productively for long stretches without checking your inbox.

Some of the most ambitious habit experiments have been conducted by corporate America. To understand why executives are so entranced by this science, consider how one of the world’s largest companies, Procter & Gamble, used habit insights to turn a failing product into one of its biggest sellers. P.& G. is the corporate behemoth behind a whole range of products, from Downy fabric softener to Bounty paper towels to Duracell batteries and dozens of other household brands. In the mid-1990s, P.& G.’s executives began a secret project to create a new product that could eradicate bad smells. P.& G. spent millions developing a colorless, cheap-to-manufacture liquid that could be sprayed on a smoky blouse, stinky couch, old jacket or stained car interior and make it odorless. In order to market the product — Febreze — the company formed a team that included a former Wall Street mathematician named Drake Stimson and habit specialists, whose job was to make sure the television commercials, which they tested in Phoenix, Salt Lake City and Boise, Idaho, accentuated the product’s cues and rewards just right.

The first ad showed a woman complaining about the smoking section of a restaurant. Whenever she eats there, she says, her jacket smells like smoke. A friend tells her that if she uses Febreze, it will eliminate the odor. The cue in the ad is clear: the harsh smell of cigarette smoke. The reward: odor eliminated from clothes. The second ad featured a woman worrying about her dog, Sophie, who always sits on the couch. “Sophie will always smell like Sophie,” she says, but with Febreze, “now my furniture doesn’t have to.” The ads were put in heavy rotation. Then the marketers sat back, anticipating how they would spend their bonuses. A week passed. Then two. A month. Two months. Sales started small and got smaller. Febreze was a dud.
The panicked marketing team canvassed consumers and conducted in-depth interviews to figure out what was going wrong, Stimson recalled. Their first inkling came when they visited a woman’s home outside Phoenix. The house was clean and organized. She was something of a neat freak, the woman explained. But when P.& G.’s scientists walked into her living room, where her nine cats spent most of their time, the scent was so overpowering that one of them gagged.

According to Stimson, who led the Febreze team, a researcher asked the woman, “What do you do about the cat smell?”

“It’s usually not a problem,” she said.

“Do you smell it now?”

“No,” she said. “Isn’t it wonderful? They hardly smell at all!”

A similar scene played out in dozens of other smelly homes. The reason Febreze wasn’t selling, the marketers realized, was that people couldn’t detect most of the bad smells in their lives. If you live with nine cats, you become desensitized to their scents. If you smoke cigarettes, eventually you don’t smell smoke anymore. Even the strongest odors fade with constant exposure. That’s why Febreze was a failure. The product’s cue — the bad smells that were supposed to trigger daily use — was hidden from the people who needed it the most. And Febreze’s reward (an odorless home) was meaningless to someone who couldn’t smell offensive scents in the first place.

P.& G. employed a Harvard Business School professor to analyze Febreze’s ad campaigns. They collected hours of footage of people cleaning their homes and watched tape after tape, looking for clues that might help them connect Febreze to people’s daily habits. When that didn’t reveal anything, they went into the field and conducted more interviews. A breakthrough came when they visited a woman in a suburb near Scottsdale, Ariz., who was in her 40s with four children. Her house was clean, though not compulsively tidy, and didn’t appear to have any odor problems; there were no pets or smokers. To the surprise of everyone, she loved Febreze.
“I use it every day,” she said.

“What smells are you trying to get rid of?” a researcher asked.

“I don’t really use it for specific smells,” the woman said. “I use it for normal cleaning — a couple of sprays when I’m done in a room.”

The researchers followed her around as she tidied the house. In the bedroom, she made her bed, tightened the sheet’s corners, then sprayed the comforter with Febreze. In the living room, she vacuumed, picked up the children’s shoes, straightened the coffee table, then sprayed Febreze on the freshly cleaned carpet.

“It’s nice, you know?” she said. “Spraying feels like a little minicelebration when I’m done with a room.” At the rate she was going, the team estimated, she would empty a bottle of Febreze every two weeks.

When they got back to P.& G.’s headquarters, the researchers watched their videotapes again. Now they knew what to look for and saw their mistake in scene after scene. Cleaning has its own habit loops that already exist. In one video, when a woman walked into a dirty room (cue), she started sweeping and picking up toys (routine), then she examined the room and smiled when she was done (reward). In another, a woman scowled at her unmade bed (cue), proceeded to straighten the blankets and comforter (routine) and then sighed as she ran her hands over the freshly plumped pillows (reward). P.& G. had been trying to create a whole new habit with Febreze, but what they really needed to do was piggyback on habit loops that were already in place. The marketers needed to position Febreze as something that came at the end of the cleaning ritual, the reward, rather than as a whole new cleaning routine.

The company printed new ads showing open windows and gusts of fresh air. More perfume was added to the Febreze formula, so that instead of merely neutralizing odors, the spray had its own distinct scent. Television commercials were filmed of women, having finished their cleaning routine, using Febreze to spritz freshly made beds and just-laundered clothing. Each ad was designed to appeal to the habit loop: when you see a freshly cleaned room (cue), pull out
Febreze (routine) and enjoy a smell that says you’ve done a great job (reward). When you finish making a bed (cue), spritz Febreze (routine) and breathe a sweet, contented sigh (reward). Febreze, the ads implied, was a pleasant treat, not a reminder that your home stinks.

And so Febreze, a product originally conceived as a revolutionary way to destroy odors, became an air freshener used once things are already clean. The Febreze revamp occurred in the summer of 1998. Within two months, sales doubled. A year later, the product brought in $230 million. Since then Febreze has spawned dozens of spinoffs — air fresheners, candles and laundry detergents — that now account for sales of more than $1 billion a year. Eventually, P.& G. began mentioning to customers that, in addition to smelling sweet, Febreze can actually kill bad odors. Today it’s one of the top-selling products in the world.

Andrew Pole was hired by Target to use the same kinds of insights into consumers’ habits to expand Target’s sales. His assignment was to analyze all the cue-routine-reward loops among shoppers and help the company figure out how to exploit them. Much of his department’s work was straightforward: find the customers who have children and send them catalogs that feature toys before Christmas. Look for shoppers who habitually purchase swimsuits in April and send them coupons for sunscreen in July and diet books in December. But Pole’s most important assignment was to identify those unique moments in consumers’ lives when their shopping habits become particularly flexible and the right advertisement or coupon would cause them to begin spending in new ways.

In the 1980s, a team of researchers led by a U.C.L.A. professor named Alan Andreasen undertook a study of peoples’ most mundane purchases, like soap, toothpaste, trash bags and toilet paper. They learned that most shoppers paid almost no attention to how they bought these products, that the purchases occurred habitually, without any complex decision-making. Which meant it was hard for marketers, despite their displays and coupons and product promotions, to persuade shoppers to change.

But when some customers were going through a major life event, like
graduating from college or getting a new job or moving to a new town, their shopping habits became flexible in ways that were both predictable and potential gold mines for retailers. The study found that when someone marries, he or she is more likely to start buying a new type of coffee. When a couple move into a new house, they’re more apt to purchase a different kind of cereal. When they divorce, there’s an increased chance they’ll start buying different brands of beer.

Consumers going through major life events often don’t notice, or care, that their shopping habits have shifted, but retailers notice, and they care quite a bit. At those unique moments, Andreasen wrote, customers are “vulnerable to intervention by marketers.” In other words, a precisely timed advertisement, sent to a recent divorcee or new homebuyer, can change someone’s shopping patterns for years.

And among life events, none are more important than the arrival of a baby. At that moment, new parents’ habits are more flexible than at almost any other time in their adult lives. If companies can identify pregnant shoppers, they can earn millions.

The only problem is that identifying pregnant customers is harder than it sounds. Target has a baby-shower registry, and Pole started there, observing how shopping habits changed as a woman approached her due date, which women on the registry had willingly disclosed. He ran test after test, analyzing the data, and before long some useful patterns emerged. Lotions, for example. Lots of people buy lotion, but one of Pole’s colleagues noticed that women on the baby registry were buying larger quantities of unscented lotion around the beginning of their second trimester. Another analyst noted that sometime in the first 20 weeks, pregnant women loaded up on supplements like calcium, magnesium and zinc. Many shoppers purchase soap and cotton balls, but when someone suddenly starts buying lots of scent-free soap and extra-big bags of cotton balls, in addition to hand sanitizers and washcloths, it signals they could be getting close to their delivery date.

As Pole’s computers crawled through the data, he was able to identify about 25
products that, when analyzed together, allowed him to assign each shopper a “pregnancy prediction” score. More important, he could also estimate her due date to within a small window, so Target could send coupons timed to very specific stages of her pregnancy.

One Target employee I spoke to provided a hypothetical example. Take a fictional Target shopper named Jenny Ward, who is 23, lives in Atlanta and in March bought cocoa-butter lotion, a purse large enough to double as a diaper bag, zinc and magnesium supplements and a bright blue rug. There’s, say, an 87 percent chance that she’s pregnant and that her delivery date is sometime in late August. What’s more, because of the data attached to her Guest ID number, Target knows how to trigger Jenny’s habits. They know that if she receives a coupon via e-mail, it will most likely cue her to buy online. They know that if she receives an ad in the mail on Friday, she frequently uses it on a weekend trip to the store. And they know that if they reward her with a printed receipt that entitles her to a free cup of Starbucks coffee, she’ll use it when she comes back again.

In the past, that knowledge had limited value. After all, Jenny purchased only cleaning supplies at Target, and there were only so many psychological buttons the company could push. But now that she is pregnant, everything is up for grabs. In addition to triggering Jenny’s habits to buy more cleaning products, they can also start including offers for an array of products, some more obvious than others, that a woman at her stage of pregnancy might need.

Pole applied his program to every regular female shopper in Target’s national database and soon had a list of tens of thousands of women who were most likely pregnant. If they could entice those women or their husbands to visit Target and buy baby-related products, the company’s cue-routine-reward calculators could kick in and start pushing them to buy groceries, bathing suits, toys and clothing, as well. When Pole shared his list with the marketers, he said, they were ecstatic. Soon, Pole was getting invited to meetings above his paygrade. Eventually his paygrade went up.

At which point someone asked an important question: How are women going
to react when they figure out how much Target knows?

“If we send someone a catalog and say, ‘Congratulations on your first child!’ and they’ve never told us they’re pregnant, that’s going to make some people uncomfortable,” Pole told me. “We are very conservative about compliance with all privacy laws. But even if you’re following the law, you can do things where people get queasy.”

About a year after Pole created his pregnancy-prediction model, a man walked into a Target outside Minneapolis and demanded to see the manager. He was clutching coupons that had been sent to his daughter, and he was angry, according to an employee who participated in the conversation.

“My daughter got this in the mail!” he said. “She’s still in high school, and you’re sending her coupons for baby clothes and cribs? Are you trying to encourage her to get pregnant?”

The manager didn’t have any idea what the man was talking about. He looked at the mailer. Sure enough, it was addressed to the man’s daughter and contained advertisements for maternity clothing, nursery furniture and pictures of smiling infants. The manager apologized and then called a few days later to apologize again.

On the phone, though, the father was somewhat abashed. “I had a talk with my daughter,” he said. “It turns out there’s been some activities in my house I haven’t been completely aware of. She’s due in August. I owe you an apology.”

When I approached Target to discuss Pole’s work, its representatives declined to speak with me. “Our mission is to make Target the preferred shopping destination for our guests by delivering outstanding value, continuous innovation and exceptional guest experience,” the company wrote in a statement. “We’ve developed a number of research tools that allow us to gain insights into trends and preferences within different demographic segments of our guest population.”

When I sent Target a complete summary of my reporting, the reply was more terse: “Almost all of your statements contain inaccurate information and publishing them
would be misleading to the public. We do not intend to address each statement point by point.” The company declined to identify what was inaccurate. They did add, however, that Target “is in compliance with all federal and state laws, including those related to protected health information.”

When I offered to fly to Target’s headquarters to discuss its concerns, a spokeswoman e-mailed that no one would meet me. When I flew out anyway, I was told I was on a list of prohibited visitors. “I’ve been instructed not to give you access and to ask you to leave,” said a very nice security guard named Alex.

Using data to predict a woman’s pregnancy, Target realized soon after Pole perfected his model, could be a public-relations disaster. So the question became: how could they get their advertisements into expectant mothers’ hands without making it appear they were spying on them? How do you take advantage of someone’s habits without letting them know you’re studying their lives?

**Before I met Andrew Pole**, before I even decided to write a book about the science of habit formation, I had another goal: I wanted to lose weight.

I had got into a bad habit of going to the cafeteria every afternoon and eating a chocolate-chip cookie, which contributed to my gaining a few pounds. Eight, to be precise. I put a Post-it note on my computer reading “NO MORE COOKIES.” But every afternoon, I managed to ignore that note, wander to the cafeteria, buy a cookie and eat it while chatting with colleagues. Tomorrow, I always promised myself, I’ll muster the willpower to resist.

Tomorrow, I ate another cookie.

When I started interviewing experts in habit formation, I concluded each interview by asking what I should do. The first step, they said, was to figure out my habit loop. The routine was simple: every afternoon, I walked to the cafeteria, bought a cookie and ate it while chatting with friends.

Next came some less obvious questions: What was the cue? Hunger? Boredom? Low blood sugar? And what was the reward? The taste of the cookie
itself? The temporary distraction from my work? The chance to socialize with colleagues?

Rewards are powerful because they satisfy cravings, but we’re often not conscious of the urges driving our habits in the first place. So one day, when I felt a cookie impulse, I went outside and took a walk instead. The next day, I went to the cafeteria and bought a coffee. The next, I bought an apple and ate it while chatting with friends. You get the idea. I wanted to test different theories regarding what reward I was really craving. Was it hunger? (In which case the apple should have worked.) Was it the desire for a quick burst of energy? (If so, the coffee should suffice.) Or, as turned out to be the answer, was it that after several hours spent focused on work, I wanted to socialize, to make sure I was up to speed on office gossip, and the cookie was just a convenient excuse? When I walked to a colleague’s desk and chatted for a few minutes, it turned out, my cookie urge was gone.

All that was left was identifying the cue.

Deciphering cues is hard, however. Our lives often contain too much information to figure out what is triggering a particular behavior. Do you eat breakfast at a certain time because you’re hungry? Or because the morning news is on? Or because your kids have started eating? Experiments have shown that most cues fit into one of five categories: location, time, emotional state, other people or the immediately preceding action. So to figure out the cue for my cookie habit, I wrote down five things the moment the urge hit:

Where are you? (Sitting at my desk.)

What time is it? (3:36 p.m.)

What’s your emotional state? (Bored.)

Who else is around? (No one.)

What action preceded the urge? (Answered an e-mail.)
The next day I did the same thing. And the next. Pretty soon, the cue was clear: I always felt an urge to snack around 3:30.

Once I figured out all the parts of the loop, it seemed fairly easy to change my habit. But the psychologists and neuroscientists warned me that, for my new behavior to stick, I needed to abide by the same principle that guided Procter & Gamble in selling Febreze: To shift the routine — to socialize, rather than eat a cookie — I needed to piggyback on an existing habit. So now, every day around 3:30, I stand up, look around the newsroom for someone to talk to, spend 10 minutes gossiping, then go back to my desk. The cue and reward have stayed the same. Only the routine has shifted. It doesn’t feel like a decision, any more than the M.I.T. rats made a decision to run through the maze. It’s now a habit. I’ve lost 21 pounds since then (12 of them from changing my cookie ritual).

After Andrew Pole built his pregnancy-prediction model, after he identified thousands of female shoppers who were most likely pregnant, after someone pointed out that some of those women might be a little upset if they received an advertisement making it obvious Target was studying their reproductive status, everyone decided to slow things down.

The marketing department conducted a few tests by choosing a small, random sample of women from Pole’s list and mailing them combinations of advertisements to see how they reacted.

“We have the capacity to send every customer an ad booklet, specifically designed for them, that says, ‘Here’s everything you bought last week and a coupon for it,’ ” one Target executive told me. “We do that for grocery products all the time.” But for pregnant women, Target’s goal was selling them baby items they didn’t even know they needed yet.

“With the pregnancy products, though, we learned that some women react badly,” the executive said. “Then we started mixing in all these ads for things we knew pregnant women would never buy, so the baby ads looked random. We’d put an ad for a lawn mower next to diapers. We’d put a coupon for wineglasses next to
infant clothes. That way, it looked like all the products were chosen by chance.

“And we found out that as long as a pregnant woman thinks she hasn’t been spied on, she’ll use the coupons. She just assumes that everyone else on her block got the same mailer for diapers and cribs. As long as we don’t spook her, it works.”

In other words, if Target piggybacked on existing habits — the same cues and rewards they already knew got customers to buy cleaning supplies or socks — then they could insert a new routine: buying baby products, as well. There’s a cue (“Oh, a coupon for something I need!”) a routine (“Buy! Buy! Buy!”) and a reward (“I can take that off my list”). And once the shopper is inside the store, Target will hit her with cues and rewards to entice her to purchase everything she normally buys somewhere else. As long as Target camouflaged how much it knew, as long as the habit felt familiar, the new behavior took hold.

Soon after the new ad campaign began, Target’s Mom and Baby sales exploded. The company doesn’t break out figures for specific divisions, but between 2002 — when Pole was hired — and 2010, Target’s revenues grew from $44 billion to $67 billion. In 2005, the company’s president, Gregg Steinhafel, boasted to a room of investors about the company’s “heightened focus on items and categories that appeal to specific guest segments such as mom and baby.”

Pole was promoted. He has been invited to speak at conferences. “I never expected this would become such a big deal,” he told me the last time we spoke.

A few weeks before this article went to press, I flew to Minneapolis to try and speak to Andrew Pole one last time. I hadn’t talked to him in more than a year. Back when we were still friendly, I mentioned that my wife was seven months pregnant. We shop at Target, I told him, and had given the company our address so we could start receiving coupons in the mail. As my wife’s pregnancy progressed, I noticed a subtle upswing in the number of advertisements for diapers and baby clothes arriving at our house.

Pole didn’t answer my e-mails or phone calls when I visited Minneapolis. I drove to his large home in a nice suburb, but no one answered the door. On my way
back to the hotel, I stopped at a Target to pick up some deodorant, then also bought some T-shirts and a fancy hair gel. On a whim, I threw in some pacifiers, to see how the computers would react. Besides, our baby is now 9 months old. You can’t have too many pacifiers.

When I paid, I didn’t receive any sudden deals on diapers or formula, to my slight disappointment. It made sense, though: I was shopping in a city I never previously visited, at 9:45 p.m. on a weeknight, buying a random assortment of items. I was using a corporate credit card, and besides the pacifiers, hadn’t purchased any of the things that a parent needs. It was clear to Target’s computers that I was on a business trip. Pole’s prediction calculator took one look at me, ran the numbers and decided to bide its time. Back home, the offers would eventually come. As Pole told me the last time we spoke: “Just wait. We’ll be sending you coupons for things you want before you even know you want them.”

Charles Duhigg is a staff writer for The Times and author of "The Power of Habit: Why We Do What We Do in Life and Business," which will be published on Feb. 28. Follow him on Twitter and on Facebook.

Editor: Joel Lovell

A version of this article appears in print on February 19, 2012, on page MM30 of the Sunday Magazine with the headline: Psst, You in Aisle 5.
A LEGAL FIGHT over the government's use of a secret surveillance tool has provided new insight into how the controversial tool works and the extent to which Verizon Wireless aided federal agents in using it to track a suspect. Court documents in a case involving accused identity thief
Daniel David Rigmaiden describe how the wireless provider reached out remotely to reprogram an air card the suspect was using in order to make it communicate with the government’s surveillance tool so that he could be located.

Rigmaiden, who is accused of being the ringleader of a $4 million tax fraud operation, asserts in court documents that in July 2008 Verizon surreptitiously reprogrammed his air card to make it respond to incoming voice calls from the FBI and also reconfigured it so that it would connect to a fake cell site, or stingray, that the FBI was using to track his location.

Air cards are devices that plug into a computer and use the wireless cellular networks of phone providers to connect the computer to the internet. The devices are not phones and therefore don’t have the ability to receive incoming calls, but in this case Rigmaiden asserts that Verizon reconfigured his air card to respond to surreptitious voice calls from a landline controlled by the FBI.

The FBI calls, which contacted the air card silently in the background, operated as pings to force the air card into revealing its location.

In order to do this, Verizon reprogrammed the device so that when an incoming voice call arrived, the card would disconnect from any legitimate cell tower to which it was already connected, and send real-time cell-site location data to Verizon, which forwarded the data to the FBI. This allowed the FBI to position its stingray in the neighborhood where Rigmaiden resided. The stingray then “broadcast a very strong signal” to force the air card into connecting to it, instead of reconnecting to a legitimate cell tower, so that agents could then triangulate signals coming from the air card and zoom-in on Rigmaiden’s location.

To make sure the air card connected to the FBI’s simulator, Rigmaiden says that Verizon altered his air card’s Preferred Roaming List so that it would accept the FBI’s stingray as a legitimate cell site and not a rogue site, and also changed a data table on the air card designating the priority of cell sites so that the FBI’s fake site was at the top of the list.
Rignmaidin makes the assertions in a 369-page document he filed in support of a motion to suppress evidence gathered through the stingray. Rignmaidin collected information about how the stingray worked from documents obtained from the government, as well as from records obtained through FOIA requests filed by civil liberties groups and from open-source literature.

During a hearing in a U.S. District Court in Arizona on March 28 to discuss the motion, the government did not dispute Rignmaidin’s assertions about Verizon’s activities.

The actions described by Rignmaidin are much more intrusive than previously known information about how the government uses stingrays, which are generally employed for tracking cell phones and are widely used in drug and other criminal investigations.

The government has long asserted that it doesn’t need to obtain a probable-cause warrant to use the devices because they don’t collect the content of phone calls and text messages and operate like pen-registers and trap-and-traces, collecting the equivalent of header information.

The government has conceded, however, that it needed a warrant in his case alone — because the stingray reached into his apartment remotely to locate the air card — and that the activities performed by Verizon and the FBI to locate Rignmaidin were all authorized by a court order signed by a magistrate.

The Electronic Frontier Foundation and the American Civil Liberties Union of Northern California, who have filed an amicus brief in support of Rignmaidin’s motion, maintain that the order does not qualify as a warrant and that the government withheld crucial information from the magistrate — such as identifying that the tracking device they planned to use was a stingray and that its use involved intrusive measures — thus preventing the court from properly fulfilling its oversight function.

“It shows you just how crazy the technology is, and [supports] all the more the need to explain to the court what they are doing,” says EFF Staff Attorney Hanni Fakhoury.
“This is more than just [saying to Verizon] give us some records that you have sitting on your server. This is reconfiguring and changing the characteristics of the [suspect’s] property, without informing the judge what’s going on.”

The secretive technology, generically known as a stingray or IMSI catcher, allows law enforcement agents to spoof a legitimate cell tower in order to trick nearby mobile phones and other wireless communication devices like air cards into connecting to the stingray instead of a phone carrier’s legitimate tower.

When devices connect, stingrays can see and record their unique ID numbers and traffic data, as well as information that points to the device’s location.

By moving the stingray around and gathering the wireless device’s signal strength from various locations in a neighborhood, authorities can pinpoint where the device is being used with much more precision than they can get through data obtained from a mobile network provider’s fixed tower location.

Use of the spy technology goes back at least 20 years. In a 2009 Utah case, an FBI agent described using a cell site emulator more than 300 times over a decade and indicated that they were used on a daily basis by U.S, Marshals, the Secret Service and other federal agencies.

The FBI used a similar device to track former hacker Kevin Mitnick in 1994, though the version used in that case was much more primitive and passive.

A 1996 *Wired* story about the Mitnick case called the device a Triggerfish and described it as “a technician’s device normally used for testing cell phones.” According to the story, the Triggerfish was “a rectangular box of electronics about a half a meter high controlled by a PowerBook” that was essentially “a five-channel receiver, able to monitor both sides of a conversation simultaneously.” The crude technology was hauled around in a station wagon and van. A black coaxial cable was strung out of the vehicle’s window to connect the Triggerfish to a direction-finding antenna on the vehicle’s roof, which had four antenna prongs that reached 30 centimeters into the sky.
The technology has become much sleeker and less obtrusive since then, but still operates under the same principles.

In Rigmaiden's case, agents apparently used two devices made by a Florida-based company called Harris. One was the company's StingRay system, which is designed to work from a vehicle driven around a neighborhood to narrow a suspect's location to a building. Once agents tracked the signals from Rigmaiden's air card to the Domicilio Apartments complex in Santa Clara, California, they apparently used another device made by Harris called the KingFish — a handheld system that allowed them to walk through the complex and zero-in on Rigmaiden's air card in apartment 1122.

Although a number of companies make stingrays, including Verint, View Systems, Altron, NeoSoft, MMI, Ability, and Meganet, the Harris line of cell site emulators are the only ones that are compatible with CDMA2000-based devices. Others can track GSM/UMTS-based communications, but the Harris emulators can track CDMA2000, GSM and iDEN devices, as well as UMTS. The Harris StingRay and KingFish devices can also support three different communication standards simultaneously, without having to be reconfigured.

Rigmaiden was arrested in 2008 on charges that he was the mastermind behind an operation that involved stealing more than $4 million in refunds from the IRS by filing fraudulent tax returns. He and others are accused of using numerous fake IDs to open internet and phone accounts and using more than 175 different IP addresses around the United States to file the fake returns, which were often filed in bulk as if through an automated process. Rigmaiden has been charged with 35 counts of wire fraud, 35 counts of identify theft, one count of unauthorized computer access and two counts of mail fraud.

The surveillance of Rigmaiden began in June 2008 when agents served Verizon with a grand jury subpoena asking for data on three IP addresses that were allegedly used to electronically file some of the fraudulent tax returns. Verizon reported back that the three IP addresses were linked to an air card account registered in the name of Travis Rupard — an identity that Rigmaiden allegedly stole. The air card was identified as a UTStarcom PC5740 device that was assigned a San Francisco Bay Area phone number.

A court order was then
submitted to Verizon Wireless requiring the company to provide historical cell site data on the account for the previous 30 days to determine what cell towers the air card had contacted and determine its general location. Verizon responded by supplying the government with information that included the latitude and longitude coordinates for five cell sites in San Jose and Santa Clara cities, in the heart of Silicon Valley.

In July, the government served Verizon Wireless with another court order directing the company to assist the FBI in the use and monitoring of a mobile tracking device to locate an unidentified suspect. The order directed Verizon Wireless to provide the FBI with any “technical assistance needed to ascertain the physical location of the [air card]....”

The government has fought hard to suppress information about how it uses stingrays, but in his motion to suppress, Rigmaiden lays out in great detail how the surveillance occurred and the nature of the technical assistance Verizon provided the FBI.

On the morning of July 14, 2008, FBI Agent Killigrew created a cell tower range chart/map consisting of a street map, plotted Verizon Wireless cell site sectors belonging to cell site Nos. 268, 139, and 279, and a triangulated aircard location signature estimate represented by a shaded area. On the chart/map, the total land area collectively covered by cell site Nos. 268, 139, and 279 is approximately 105,789,264 ft². FBI Agent Killigrew used triangulation techniques and location signature techniques to eliminate 93.9% of that 105,789,264 ft² area resulting in the location estimate being reduced to 6,412,224 ft² represented by the shaded area. The shaded area on the cell tower range chart covers the location of apartment No. 1122 at the Domicilio apartment complex.

On July 15, agents with the FBI, IRS and US Postal Service flew to San Jose to triangulate Rigmaiden’s location using the stingray. They worked with technical agents from the San Francisco FBI’s Wireless Intercept and Tracking Team to conduct the real-time tracking.
According to Rigmaiden, the agents drove around the cell site areas gathering information about signal range and radio frequencies for each cell site sector. “The radio frequency information was needed so that the FBI technical agents could properly configure their StingRay and KingFish for use in cell site emulator mode,” Rigmaiden writes. “By referencing a list of all the radio frequencies already in use, the FBI was able to choose an unused frequency for use by its emulated cellular network that would not interfere with the various FCC licensed cellular networks already operating in the noted area.”

The next day, Verizon Wireless surreptitiously reprogrammed Rigmaiden’s air card so that it would recognize the FBI’s stingray as a legitimate cell site and connect to it “prior to attempting connections with actual Verizon Wireless cell sites.” The FBI needed Verizon to reprogram the device because it otherwise was configured to reject rogue, unauthorized cell sites, Rigmaiden notes.

On July 16, the FBI placed 32 voice calls to the air card between 11am and 5pm. Each time the air card was notified that a call was coming in, it dropped its data connection and went into idle mode. At the same time, it sent real-time cell site location information to Verizon, which forwarded the information to the FBI’s DCS-3000 servers, part of the elaborate digital collection system the FBI operates for wiretapping and pen-registers and trap-and-traces. From the FBI’s servers, the location data was transmitted wirelessly through a VPN to the FBI’s technical agents “lurking in the streets of Santa Clara” with the StingRay.
At this point, the StingRay took over and began to broadcast its signal to force the air card — and any other wireless devices in the area — to connect to it, so that agents could zoom-in on Rigmaiden’s location.

“Because the defendant attempted to keep his aircard continuously connected to the Internet, the FBI only had a very short window of time to force the aircard to handoff its signal to the StingRay after each surreptitious voice call [and] the FBI needed to repeatedly call the aircard in order to repeatedly boot it offline over the six hours of surreptitious phone calls,” Rigmaiden writes. “Each few minute window of time that followed each denial-of-service attack (i.e., surreptitious phone call) was used by the FBI to move its StingRay, while in cell site emulator mode, to various positions until it was close enough to the aircard to force an Idle State Route Update (i.e., handoff).”

Rigmaiden maintains that once the connection was made, the StingRay wrote data to the air card to extend the connection and also began to “interrogate” the air card to get it to broadcast its location. The FBI used the Harris AmberJack antenna to deliver highly-directional precision signals to the device, and moved the StingRay around to various locations in order to triangulate the precise location of the air card inside the Domicilio Apartments complex.

According to Rigmaiden, agents also transmitted Reverse Power Control bits to his air card to get it to transmit its signals at “a higher power than it would have normally transmitted if it were accessing cellular service through an actual Verizon Wireless cell site.”

Once agents had tracked the device to the Domicilio Apartments complex, they switched out the StingRay for the handheld KingFish device to locate Rigmaiden’s apartment within the complex.

Around 1am on July 17, an FBI agent sent a text message to another FBI agent stating, “[w]e are down to an apt
complex....” By 2:42 am, one of the FBI technical agents sent a text message to someone stating that they had “[f]ound the card” and that agents were “working on a plan for arrest.”

Agents still didn’t know who was in the apartment — since Rigmaiden had used an assumed identity to lease the unit — but they were able to stake out the apartment complex and engage in more traditional investigative techniques to gather more intelligence about who lived in unit 1122. On August 3, while the apartment was still under surveillance, Rigmaiden left the unit. Agents followed him a short distance until Rigmaiden caught on that he was being followed. After a brief foot chase, he was arrested.

Rigmaiden and the American Civil Liberties Union and Electronic Frontier Foundation have argued that the government did not obtain a legitimate warrant to conduct the intrusive surveillance through the stingray. They say it’s indicative of how the government has used stingers in other cases without proper disclosure to judges about how they work, and have asked the court to suppress evidence gathered through the use of the device.

U.S. District Court Judge David Campbell is expected to rule on the motion to suppress within a few weeks.
The National Security Agency has secretly broken into the main communications links that connect Yahoo and Google data centers around the world, according to documents obtained from former NSA contractor Edward Snowden and interviews with knowledgeable officials.

By tapping those links, the agency has positioned itself to collect at will from hundreds of millions of user accounts, many of them belonging to Americans. The NSA does not keep everything it collects, but it keeps a lot.

According to a top-secret accounting dated Jan. 9, 2013, the NSA’s acquisitions directorate sends millions of records every day from internal Yahoo and Google networks to data warehouses at the agency’s headquarters at Fort Meade, Md. In the preceding 30 days, the report said, field collectors had processed and sent back 181,280,466 new records — including “metadata,” which would indicate who sent or received e-mails and when, as well as content such as text, audio and video.

The NSA’s principal tool to exploit the data links is a project called MUSCULAR, operated jointly with the agency’s British counterpart, the Government Communications Headquarters. From undisclosed interception points, the NSA and the GCHQ are copying entire data flows across fiber-optic cables that carry information among the data centers of the Silicon Valley giants.

The infiltration is especially striking because the NSA, under a separate program known as PRISM, has front-door access to Google and Yahoo user accounts through a court-approved process.
The MUSCULAR project appears to be an unusually aggressive use of NSA tradecraft against flagship American companies. The agency is built for high-tech spying, with a wide range of digital tools, but it has not been known to use them routinely against U.S. companies.

In a statement, the NSA said it is “focused on discovering and developing intelligence about valid foreign intelligence targets only.”

“NSA applies Attorney General-approved processes to protect the privacy of U.S. persons — minimizing the likelihood of their information in our targeting, collection, processing, exploitation, retention, and dissemination,” it said.

In a statement, Google’s chief legal officer, David Drummond, said the company has “long been concerned about the possibility of this kind of snooping” and has not provided the government with access to its systems.

“We are outraged at the lengths to which the government seems to have gone to intercept data from our private fiber networks, and it underscores the need for urgent reform,” he said.

A Yahoo spokeswoman said, “We have strict controls in place to protect the security of our data centers, and we have not given access to our data centers to the NSA or to any other government agency.”

Under PRISM, the NSA gathers huge volumes of online communications records by legally compelling U.S. technology companies, including Yahoo and Google, to turn over any data that match court-approved search terms. That program, which was first disclosed by The Washington Post and the Guardian newspaper in Britain, is authorized under Section 702 of the FISA Amendments Act and overseen by the Foreign Intelligence Surveillance Court (FISC).

Intercepting communications overseas has clear advantages for the NSA, with looser restrictions and less oversight. NSA documents about the effort refer directly to “full take,” “bulk access” and “high volume” operations on Yahoo and Google networks. Such large-scale collection of Internet content would be illegal in the United States, but the operations take place overseas, where the NSA is allowed to presume that anyone using a foreign data link is a foreigner.

Outside U.S. territory, statutory restrictions on surveillance seldom apply and the FISC has no jurisdiction. Senate Intelligence Committee Chairman Dianne Feinstein (D-Calif.) has acknowledged that Congress conducts
little oversight of intelligence-gathering under the presidential authority of Executive Order 12333, which defines the basic powers and responsibilities of the intelligence agencies.

John Schindler, a former NSA chief analyst and frequent defender who teaches at the Naval War College, said it is obvious why the agency would prefer to avoid restrictions where it can.

“Look, NSA has platoons of lawyers, and their entire job is figuring out how to stay within the law and maximize collection by exploiting every loophole,” he said. “It’s fair to say the rules are less restrictive under Executive Order 12333 than they are under FISA,” the Foreign Intelligence Surveillance Act.

In a statement, the Office of the Director of National Intelligence denied that it was using executive authority to “get around the limitations” imposed by FISA.

The operation to infiltrate data links exploits a fundamental weakness in systems architecture. To guard against data loss and system slowdowns, Google and Yahoo maintain fortresslike data centers across four continents and connect them with thousands of miles of fiber-optic cable. Data move seamlessly around these globe-spanning “cloud” networks, which represent billions of dollars of investment.

For the data centers to operate effectively, they synchronize large volumes of information about account holders. Yahoo’s internal network, for example, sometimes transmits entire e-mail archives — years of messages and attachments — from one data center to another.

Tapping the Google and Yahoo clouds allows the NSA to intercept communications in real time and to take “a retrospective look at target activity,” according to one internal NSA document.

To obtain free access to data-center traffic, the NSA had to circumvent gold-standard security measures. Google “goes to great lengths to protect the data and intellectual property in these centers,” according to one of the company’s blog posts, with tightly audited access controls, heat-sensitive cameras, round-the-clock guards and biometric verification of identities.

Google and Yahoo also pay for premium data links, designed to be faster, more reliable and more secure. In recent years, both of them are said to have bought or leased thousands of miles of fiber-optic cables for their own exclusive use. They had reason to think, insiders said, that their private, internal networks were safe from prying eyes.
In an NSA presentation slide on “Google Cloud Exploitation,” however, a sketch shows where the “Public Internet” meets the internal “Google Cloud” where their data reside. In hand-printed letters, the drawing notes that encryption is “added and removed here!” The artist adds a smiley face, a cheeky celebration of victory over Google security.

Two engineers with close ties to Google exploded in profanity when they saw the drawing. “I hope you publish this,” one of them said.

For the MUSCULAR project, the GCHQ directs all intake into a “buffer” that can hold three to five days of traffic before recycling storage space. From the buffer, custom-built NSA tools unpack and decode the special data formats that the two companies use inside their clouds. Then the data are sent through a series of filters to “select” information the NSA wants and “defeat” what it does not.

PowerPoint slides about the Google cloud, for example, show that the NSA tries to filter out all data from the company’s “Web crawler,” which indexes Internet pages.

According to the briefing documents, prepared by participants in the MUSCULAR project, collection from inside Yahoo and Google has produced important intelligence leads against hostile foreign governments that are specified in the documents.

Last month, long before The Post approached Google to discuss the penetration of its cloud, Eric Grosse, vice president for security engineering, said the company is rushing to encrypt the links between its data centers. “It’s an arms race,” he said then. “We see these government agencies as among the most skilled players in this game.”

Yahoo has not announced plans to encrypt its data-center links.

Because digital communications and cloud storage do not usually adhere to national boundaries, MUSCULAR and a previously disclosed NSA operation to collect Internet address books have amassed content and metadata on a previously unknown scale from U.S. citizens and residents. Those operations have gone unchallenged in public or in Congress because their existence was classified.

The Google and Yahoo operations call attention to an asymmetry in U.S. surveillance law. Although Congress has lifted some restrictions on NSA domestic surveillance on grounds that purely foreign communications sometimes pass over U.S. switches and cables, it has not added restrictions overseas, where American communications or
data stores now cross over foreign switches.

“Thirty-five years ago, different countries had their own telecommunications infrastructure, so the division between foreign and domestic collection was clear,” Sen. Ron Wyden (D-Ore.), a member of the intelligence panel, said in an interview. “Today there’s a global communications infrastructure, so there’s a greater risk of collecting on Americans when the NSA collects overseas.”

It is not clear how much data from Americans is collected and how much of that is retained. One weekly report on MUSCULAR says the British operators of the site allow the NSA to contribute 100,000 “selectors,” or search terms. That is more than twice the number in use in the PRISM program, but even 100,000 cannot easily account for the millions of records that are said to be sent to Fort Meade each day.

In 2011, when the FISC learned that the NSA was using similar methods to collect and analyze data streams — on a much smaller scale — from cables on U.S. territory, Judge John D. Bates ruled that the program was illegal under FISA and inconsistent with the requirements of the Fourth Amendment.

Soltani is an independent security researcher and consultant.

Barton Gellman writes for the national staff. He has contributed to three Pulitzer Prizes for The Washington Post, most recently the 2014 Pulitzer Prize for Public Service.

PROMOTED STORIES

McCain: U.S. should spurn Russia rocket engines

Millions of Millennials making Millions

Your 401k Isn't Growing as Fast as It Should - Here's Why

Recommended by

Reuters

BBC News

Mint.com

https://www.washingtonpost.com/world/national-security/nsa-infiltr...nts-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html
16 Celebs You Had No Clue Were Married To Each Other
Entertainment - Answers.com

This drone is packing heat, but it isn't breaking any laws.
Fortune

Man fulfills a promise made during WWII
CNN