2
DATA REVOLUTION

CHARLES MORGAN SLIPPED THE GEARSHIFT into first and pushed the accelerator to the floor. He quickly sped up, revving the powerful engine close to its maximum 9,000 rpms. With just days to go before one of the last big events of his race career, Morgan was putting the million-dollar Ferrari through its paces, at close to 200 miles per hour.

The bright red race car was an engineering marvel, a twelve-cylinder rocket that rode just inches above the track at Sebring, Florida. Its curves flowed back and up over the wheels like a low wave. A spoiler in the shape of a T on the tail end helped keep the car pressed to the roadway. On its side was the word ACXIOM in bold letters.

Unlike a lot of companies that sponsor race cars, Acxiom is not a household name. But as a billion-dollar player in the data industry, with details about nearly every adult in the United States, it has as much reach into American life as Pepsi or Goodyear. You may not know about Acxiom, but it knows a lot about you.

Morgan, Acxiom's chief executive, has made racing a central part of his life, and in this event he was aiming for his twentieth road race victory. It is an expensive hobby, but also the fulfillment of his teenage dream: To be the man in the driver seat instead of watching from the grandstands. Keeping the Acxiom Ferrari on the road cost up to $200,000 annually. He spent millions more on racing in general, including his son's racing operation. Morgan could afford it, though, because he has made a fortune at Acxiom by leading the collection, management, and high-tech packaging of personal information.

He was not thinking about data on this warm-up day, in March 1997. He was concentrating on the track's familiar curves, the bumpy surface jostling him from side to side, his hands on the small steering wheel, his elbows bent down. Morgan hoped the car would propel him and three teammates to victory in the grueling and prestigious twelve-hour race ahead. He thought, If only we can keep the racing machine on track. Suddenly, Morgan spun out. He nicked a wall and shattered part of the car's sleek carbon fiber shell. As the team repairs the damage, they blame the mishap on cold tires with a loose grip on the road. It's an excuse often allowed for self-funded part-time racers like Morgan, guys sometimes known in the business as "gentlemen drivers."

Things seem to go better on race day, as Morgan whips around the track. After some initial troubles, he gains on the leaders. Then he is cut off by a rival heading into the pits. Morgan slams into the car, a Porsche, and breaks his right hand.

Afterward, Morgan shrugged it off. "If I were doing something really risky, I'd be racing planes or offshore boats or Indy cars. This isn't that dangerous. Really," he told a *Success* magazine writer for a story at the time. "Of course, if I stuck you in the car and took you around for a lap, you'd probably wet your pants."

TO GET TO THE PLACE where Charles Morgan made his fortune, you must drive through the forested hills north of Little Rock, Arkansas, and then along the dense commercial strip of asphalt that cuts through the small city of Conway.

Conway is a former railroad town with three colleges. Like Acxiom, the city has grown a lot in recent years, and now parts of it are overrun by fast-food restaurants, strip malls, and congestion. Despite the changes, the Acxiom campus remains a source of community pride, and Morgan something of a local hero. The company is Conway's largest employer. Because it attracts so many bright people, Acxiom also boosts the education levels of the city's adult population far above the average of one of the nation's poorly educated states. Morgan donated millions to Hendrix College, a liberal arts school in town.

Acxiom's low-slung brick buildings spread out across a campus along Dave Ward Drive, a busy road named after a local bus manufacturer whose son founded the company in 1969. Behind the modest facade are scores of powerful computers containing one of the richest collections of personal and confidential information in the world.

You enter computer center A by passing a reception area, going through a secure door, and walking up a ramp into a large air-conditioned space with a dropped ceiling and fluorescent lights. Pallets of supplies sit on the floor. In the early days, this room was the entire company, complete with executives' desks, a printing facility, and computers exhaling hot air. Now it is simply a data powerhouse. Beneath the floors snake miles of cables that connect the computers to one another and to the rest of the world. All day long, every day of the year, those cables transmit information about Americans to and from Acxiom. It's not just names, ages, addresses, and telephone numbers. The computers in these rooms also hold billions of records about marital status and families and the ages of children. They track individuals' estimated incomes, the value of their homes, the make and price of their cars. They maintain unlisted phone numbers and details about people's occupations, religions, and ethnicities. They sometimes know what some people read, what they order over the phone and online, and where they go on vacation. These are details Acxiom gently refers to as "purchase behavior and lifestyle data." But there's more.

A short walk to another building brings you to rooms with newer computers, machines that occupy far less space and hold vastly more information. It's easy to see on the tile floor where the older equipment stood. The new computers operate in spare black boxes that look like high-end Sub-Zero refrigerators. For security reasons, Acxiom does not identify the client information in each of the computers. Instead, the machines are labeled with a series of motifs. Some sport pictures of muscle cars, such as Mustangs and Firebirds. Others display characters from *SpongeBob Squarepants* or *Sesame Street*. Shark fins sit atop one group of machines that happen to hold tens of millions of financial records.

In all, Acxiom's electronic storehouses in Conway can hold what's called a petabyte of information, or a thousand trillion bytes. Grasping the meaning of that quantity is challenging, even for mathematicians or computer scientists. You might do slightly better thinking of it roughly as a 50,000-mile-high stack of King James Bibles. Just one part of this digital ocean, a core service that Acxiom calls InfoBase, comprises the largest collection of U.S. consumer and telephone data available in one source, according to company documents.

Many companies in the United States maintain data centers now, operations that became a central if little understood part of American life during the 1990s and at the start of the twenty-first century. These companies are altering the nature of business and, in some ways, our country. Working on a network of supercomputers—something Acxiom calls "grid computing"—the company systematically matches and analyzes the information it collects to create fine-grained portraits about roughly 200 million adults. Every one of them is labeled with a 16-digit code unique to each person to make the processing of their records swifter.

The company helps retailers such as Lands' End focus their catalogues, banking customers like Citigroup profile individuals for credit offers, and insurers such as Allstate decide whom to serve and whom to exclude. It manages billions of financial and personal records for the privately owned credit bureau Trans Union. It enables drug companies to target people with certain ailments. It screens people for jobs and helps track down debtors. It outlines and predicts behavior.

And since September 11, 2001, Acxiom has offered its technical know-how and raw material—the details about you, your life, and your family—to some of the largest surveillance and screening systems ever devised by the U.S. government.

NEAR THE CENTER OF THE CONWAY CAMPUS is a cinder-block room. It has durable carpet in it now and rows of desks and PCs for the administrative staff that's housed there. In the mid-1970s, this space was the garage where Morgan tinkered with his first race cars, during breaks from long hours in the computer room. One hour he might be writing code and the next his hands would be black with grease.

Morgan and his company didn't set out to be pioneering. After getting a mechanical engineering degree from the University of Arkansas, he worked for a time at IBM in the 1960s as a systems engineer. But he wanted to take his own risks, build his own company, make money, and have time to race. So in 1972 he moved to Demographics in Conway, the company that would become Acxiom.

Morgan is a native Arkansan, tall and thin, who favors wireless glasses and custom-made clothes. He likes his Jack Daniel's neat, listens to Barbra Streisand, and speaks with a twang. While giving a deposition a few years ago, he referred to an opposing lawyer he'd just met as "buddy." When he grew frustrated with questions about Acxiom's business, he said, "I mean, I'm really in a hurt here."

When he joined Demographics, an ardent Democrat named Charles Ward—owner of the Ward School Bus Manufacturing Company—wanted to use computer technology to help the Democratic National Committee raise money. Relying on voter registration lists, staff at Demographics figured out a way to pick out individuals who seemed most likely to write checks for local and regional candidates. They employed mainframe computers—sophisticated machines for the time—that were programmed with manila-colored punch cards. Among those they helped was Dale Bumpers, the governor of Arkansas who went on to become a U.S. senator and would later serve as an Acxiom lobbyist in Washington. The Demographics approach represented a big leap for political fund-raising, because it enabled candidates to far more efficiently select targets likely to give them cash.

It was an up and down business. Fund-raising was seasonal, dependent on the election cycles. The clients were sometimes frugal and often didn't pay on time. As a consequence, Demographics occasionally couldn't meet its payroll. "There were weeks when we had to float it," Morgan would say later. "And one year we had to put our executives on half salary." But the lessons Morgan and his colleagues absorbed proved invaluable. They learned how to make money by collecting, managing, and massaging information about businesspeople, housewives, graduate students, and immigrants—indeed, potential spenders everywhere. By the mid-1970s, they had come up with a brash idea: To use computers and heaps of information about people to help marketers get to know individuals better. It was a plan that would help fuel a data and marketing revolution at the end of the twentieth century—and raise new questions about what it means to live a private life in America.

Their first customer was the American Bible Society, which was looking for ways to boost donations. The Bible Society executive who arranged the deal, a New Yorker, was amazed at the high-tech operation in Arkansas. "She was dumbfounded to find this building out in the middle of a field with cows grazing immediately behind the building. She had been there about a few minutes and said, 'I gotta call my boss. He is not going to believe this,'" Morgan would say almost two decades after the fact. "She literally starts shrieking and saying, 'Joe, you can't believe it. There are cows here right outside the door here.'"

The transformation from political fund-raiser to direct marketer would make Morgan wealthy. In 1972, Charles Ward was having financial difficulties. He offered Morgan a chance to buy a stake in the company, which brought in about $400,000 in revenue that year. For $50,000, Morgan got half. Acxiom is now a $1 billion, publicly held company. With more than 4 million shares in June 2003, worth some $60 million and rising, Morgan was the single largest individual shareholder.

GATHERING AND MERGING INFORMATION about people isn't new. Throughout the twentieth century, marketers, lenders, insurers, private investigators, and of course the government continually came up with efforts to collect or traffic in names, addresses, and individuals' activities.

For marketers, it was a matter of finding people who might be most interested in their products. Banks and others wanted to track down debtors. For some, the list building was politically motivated, as when the government tracked labor activists or people who criticized World War I. Such efforts became rampant during the fifties and sixties, when the FBI, the Army, and shadowy conservative groups such as the Church League created dossiers about tens of thousands of students, anti-war activists, social crusaders, and others deemed undesirable.

Information compilers have always found relatively little standing in the way of these efforts. The laws didn't exist or were too weak to matter or they were simply ignored. Dossier builders were limited only by what their minds and file cabinets could hold. The creation of the computer in the 1940s was a boon to these kinds of initiatives. Simple and slow as they were, the early electronic brains spurred a new way of thinking about information. In just a few years, businesses, bureaucrats, and scientists realized they had the tool of their dreams: machines that could store more information and help answer more questions than ever before.

By the early sixties, some 250 businesses began specializing in brokering almost any details they could acquire. Fueling this nascent industry were magazine publishers, hoteliers, car dealerships, and other businesspeople, who soon understood they could make extra cash just by selling the names, addresses, and preferences of their regular customers. One of the notable leaders was a firm called the Dunhill International List Company. In 1964, it sold private details about people to magazine publishers and others who wanted to target their pitches. For $14, you could acquire the names of a thousand women who had bought a "bust developer" product. If you wanted to find "men and women of large means," the list cost $15. A few dollars more would get you the names and addresses of newlyweds, 500,000 in all.

It wasn't long before government agencies also got into the business. Clerks across the country began selling lists of births, marriages, new families, and tax rolls to companies like Dunhill. For some companies, information brokering became big business. The Reuben H. Donnelley Corporation became a regular buyer of information about the cars people registered. Before long, it was selling access to lists of 400,000 car owners.

The muckraking journalist Vance Packard estimated that by 1964 businesses, charities, and political groups were spending $400 million annually to buy information about individuals. Until the laws were changed, one city clerk earned the grand sum of $60,000 selling details about couples applying for marriage licenses. "There's no question about it," Packard wrote at the time, in a book called *The Naked Society*. "In bulk, we are very attractive." Increases in computing power enabled the industry to expand throughout the decade. On the leading edges of this growth in data collection were credit bureaus, hundreds of operations across the country that conducted background checks of individuals on behalf of credit card issuers and other lenders. They first gathered information from the person seeking credit. The bureaus added in their own data collected from credit issuers, newspapers, and public records. When that wasn't enough, they sent out investigators to knock on doors. These commercial gumshoes collected innumerable anecdotes from landlords, friends, neighbors, and coworkers. Most of the time, because they faced quotas, the investigators didn't have time to verify the stories. In a way that seems quaint now, an analyst, a real person, then took stock of the applicant's report before passing judgment.

A major force at the time was the Atlanta-based Retail Credit Company, later to become Equifax. It had some seven thousand investigators who compiled information on some 45 million adults. Retail Credit's customers included insurers and employers, and its reports could be unsettlingly specific. One credit report, for instance, described a retired Army lieutenant colonel as "a rather wild-tempered, unreasonable, and uncouth person who abused his rank and wasn't considered a well-adjusted person."

The bureaus insisted they handled such reports with care, making the same promises they make now: No one gets access to the information unless they have signed contracts limiting the use of the reports to credit granting. The reality, then as now, is that anyone intent on getting those reports had no trouble at all, generally for a small fee, sometimes for nothing.

This bonanza of information spurred the creation of new conveniences that we now take for granted. Instant credit, cheaper mortgages, a panoply of shopping options, and even detailed and accurate phone books. But it also was a huge step down the slippery slope of privacy encroachment for commercial gain. In 1971, a Michigan University academic named Arthur R. Miller caught the zeitgeist when he described the computer-driven changes as a "cybernetic revolution." His book was called *The Assault on Privacy.*

"The new information technologies seem to have given birth to a new social virus—'data-mania,'" Miller wrote. "We must begin to realize what it means to live in a society that treats information as an economically desirable commodity and a source of power."

• • •

FOR ALL HIS PRESCIENCE, Miller, now a law professor at Harvard, had no idea just how fast and how much personal information the world would create. Only science fiction writers really had the gall to suggest the pending magnitude of change. "In a very few generations—computer generations—which by this time may last only a few months—there will be a mental explosion; the merely intelligent machine will swiftly give way to the ultra-intelligent machine," wrote Arthur Clarke, in a 1968 *Playboy* magazine article.

An effect known as Moore's Law was driving the revolution. The eponymous Gordon Moore was co-founder of Intel, the computer chip maker. In the mid-1960s, Moore noticed that the power of the chips doubled every year. He predicted correctly the phenomenon would continue. By the early nineties, the power of computer processors exploded and the cost of data storage was sliding fast. The Internet, the global computer network developed by the Defense Department and embraced by the academic world, was becoming commonplace. Suddenly companies like Acxiom could more easily employ systems known as data warehouses, to hold the information, and data mining, to make sense of it. Instead of creating a simple list of people who bought, say, an Oldsmobile or read the *Saturday Evening Post,* Acxiom had the data savvy and computer power to combine dozens of characteristics about people.

The resulting profiles, generated by statistical models, enabled the company to better predict what people were likely to buy or do. The Internet became both the conduit for gathering data and the instantaneous delivery system. Companies could now know who you were the instant you called. "Imagine if you could obtain an instant consumer profile of each prospect at your first contact," gushed Acxiom's promotional material about the InfoBase Profiler system.

By 2004, the company had developed its grid supercomputing system, enabling its analysts to do everything faster and with far more depth. Marty Abrams, a former executive at Experian, the giant credit bureau, and a leading thinker about data policy issues, likened the technological changes to the upheaval caused by Henry Ford's assembly-line innovations or the steam engine. "It's like the revolution that occurred when we began to understand the world was round, and not flat."

Technology forecaster Paul Saffo, director of the Institute for the Future, liked to cite a toy popular a few years ago called the Furby. Using a microchip, the Furby recorded speech and appeared to talk. But far from being just a fuzzy toy, the Furby represented a technological transformation, because it had more computing power inside it than the first Apollo lunar module. That kind of power, coupled to the Internet, made it easier than ever before for one person to find out information about another. "It used to take an army of gumshoes to do what an individual can do clicking their keyboards in a matter of minutes," Saffo said.

Researchers at the University of California at Berkeley concluded that all the information collected by humanity through 1999 would more than double in the next several years—and continue to grow at an accelerating pace. That's approximately a dozen exabytes by the Berkeley team's reckoning. Just five exabytes equals all the words ever spoken. Most of this information comes in the form of benign, even banal office documents and memos that go into someone's computer and never disappear. Much of it is duplicative. But an extraordinary amount—far beyond most people's reckoning—is the telling minutiae of individuals' lives, their families, whereabouts, habits, and shopping predilections.

For more than a decade, Acxiom and its allies and competitors were, by their own account, in a sort of feeding frenzy. Acxiom alone had almost 1 million times the capacity for information in 2004 than it had in 1983, the year it first sold shares of stock in the company. Just one of its sleek black computers holds roughly the equivalent of 5 million copies of *Huckleberry Finn.*

Much of the information that Acxiom manages and enhances comes from technology-savvy (and very data-hungry) retailers like Sears, Roebuck, gift shop chains like Hallmark Cards, grocery stores such as Safeway, scores of mail-order operations like Lands' End and the publisher Rodale. Nearly all the top banks and credit card companies send data to Acxiom, including Bank One Financial Services, Bank of America, MBNA America Bank, and Charles Schwab. That holds true also for GM and Toyota, AT&T and other telephone companies, Pfizer and fellow drugmakers, Microsoft and IBM. They all have collected massive amounts of information about their customers, and they all work with Acxiom to learn still more about what makes their customers tick.

During a tour of Acxiom's Conway campus several years ago, Morgan paused, turned to a visitor, and, over the loud hum of the machines, marveled about what was happening. "They have gone on an information collecting binge," Morgan said about the commercial world. "There's just this insatiable appetite for more information.

"They record everything about their customers," Morgan said. "They're saying, 'We ought to convince customers this is good for them.'"

Helping businesses make sense of all this information became one of Acxiom's main goals in the 1990s. Simple lists weren't good enough anymore. But profiling people well, getting inside their heads, meant acquiring even more information about them. Acxiom began making deals with both clients and competitors. These companies underscore the breadth of the data revolution and the wealth of information they collect.

At the beginning of the nineties, Acxiom cut a deal with one of the nation's largest direct mailers, ADVO-System Inc., a little known firm that at the time delivered weekly pitches to some 52 million households. Under the arrangement, the two shared technology and information, including the names, addresses, and other information from ADVO-System computers. ADVO-System bought half of Acxiom's InfoBase. Another partner was R. L. Polk & Co., one of the oldest information services in the country and one of the few that has grown as large or as powerful as Acxiom. The cornerstone of its business is "automotive intelligence" about car owners. It also led the way in the race to build up massive amounts of lifestyle and buying information. In promotional material not long ago, Polk declared that "Information is power." Acxiom signed a long-term agreement to manage Polk's data.

In 1996, Acxiom bought Direct Media Inc., the nation's biggest list manager and broker, a Goliath that processed more than 10 percent of all third-class junk mail—hundreds of millions of pieces a year. The list of other contributors over the years to InfoBase—the service Acxiom claims is the largest of its kind in America—reads like a who's who of data compilers: DataQuick List Service, Partners' Marketing, American Data Resources, I Rent America.

One deal involved a handshake between Acxiom and a company called Abacus Direct Corp., a consortium of retailers who share information about their customers in a cooperative database. The deal signaled a momentous change for individuals, people the industry refers to as "consumers." Not only were the two companies going to share information, they were going to apply cutting-age behavior modeling to every individual. In May 1999 the companies described their partnership: "Under terms of the agreement, Abacus will maximize the power of its Alliance database, the nation's largest database of consumer catalog buying behavior, in conjunction with Acxiom's InfoBase database, the nation's premier source for demographic information, to create new, jointly marketed data products."

Just weeks before, a partnership was announced between Abacus and HNC Software, a company that specializes in artificial intelligence software. HNC can analyze billions of transactions and learn from them to predict what an individual is likely to do. It watches, for example, every credit card transaction for some companies, learns individuals' spending patterns, and tracks any anomalies, in part to root out fraud. "Under the agreement," the companies proclaimed, "Abacus will use HNC's Content Mining technology to enhance the data mining of billions of mail order merchandise purchasing transactions maintained within the proprietary Abacus Alliance database of 88 million households. In turn, HNC Financial Solutions plans to apply the Abacus aggregate prior purchasing data to further enhance the value of HNC Financial Solutions products to its clients."

This was a new kind of marketing surveillance, an emerging power that excited marketers no end. Richard Barton, a lawyer for the Direct Marketing Association, was one of many in the industry who watched all of this unfold with pride. "We have the capability to gather, store, analyze, segment and use for commercial (and many other) purposes more data about more people than was ever dreamed of," he boasted to a trade magazine. "And technology is providing us with even more ingenious ways to reach into the lives of every American."

Most individuals had no idea this was happening.

FEW OTHER PARTNERS have been as important to Acxiom as the one created by the Union Tank Car Company, a railway car leasing firm that created a holding operation called Trans Union.

Trans Union has always been in a hurry to grow. It bought the Credit Bureau of Cook County, which had maintained 3.6 million files in hundreds of file cabinets. In 1972, the fledgling company made a bold claim for a system it called the Credit Reporting Online Network Utility System, better known in industry circles as CRONUS. By the company's own reckoning, CRONUS "revolutionized the credit reporting system" by giving lenders a look at borrowers online more than two decades before the advent of the World Wide Web.

Trans Union fought its way to the top tier of a deeply competitive industry, embracing computers, networks, and other data processing technology. It bought out competitors, and because it was a privately held company, it had to answer only to its owners. By the early 1990s, Trans Union had become a national credit bureau, with information in its files about almost every American adult—at least those who weren't living in mountain cabins without electricity or credit cards.

Trans Union wanted Acxiom to help work with banking customers to target people who, based on data profiles, might be likely to sign up for credit cards. It also wanted to improve its use of data, and figured Acxiom could be a partner in developing new technology. At Trans Union's helm was Harry Gambill, a graduate of Arkansas State University who knew Charles Morgan personally. Morgan realized that his technology and information, coupled with Trans Union's fountain of personal data, could be enormously profitable. In 1992, the two companies made a deal that would help both of them expand their businesses. This sort of arrangement, played out across the financial and data industry, would dramatically accelerate the collection of personal information in the coming years.

Trans Union is one of Acxiom's closest partners. The deal in July 1992 called for Acxiom to acquire all of Trans Union's interest in its Chicago data center. Acxiom would then manage Trans Union's information and the two would work together to develop technology and services enabling them to better profile and target individuals. They would market and assess such individuals for risk, to better discriminate between profitable customers and those who should be ignored.

Acxiom agreed also to "use its best efforts to cause two people designated by Trans Union to be elected to Acxiom's board of directors." No one will say precisely how much stock Trans Union got out of the deal. Two years later, Acxiom added tens of thousands of square feet to the Conway facility to accommodate the growing amount of information it was handling for Trans Union. Over the last decade, the ties have grown stronger. In 2002, the two companies' sales forces decided to market their products together. A short time later, Acxiom paid almost $35 million for Trans Union's background screening business. For its part, Trans Union paid Acxiom more than $71 million in 2003, up from $50.6 million the year before. When pressed about the relationship at the end of 2003, Morgan acknowledged it was a close one. "We run their computers. We are the computer operators. We do the systems programming," he said about the fabled CRONUS. "We are responsible for the computer infrastructure."

THE BIBLE OF MAILING LISTS in America is a $331 document called the *SRDS Direct Marketing List Source*. Not too long ago it was the size of a telephone book for a small city. In the early 2000s, it became a multivolume document that resembles an engorged directory for New York City and Los Angeles combined.

In 1,600 pages of fine print, volume 2 of the *List Source* offers marketers' names, ages, addresses, and other details about book buyers, magazine readers, muscle car owners in Florida, and people who buy prints online from the Metropolitan Museum of Art. It has a list called Gay America Megafile with almost 700,000 names. Other lists contain the names of millions of parents and children. Marketers buy these lists, create files of the best "prospects," and go at them with direct mail, email pitches, and telemarketing calls. Direct mail, a.k.a. junk mail, lists have been around for decades, of course, but year by year they become richer, more arcane, and potentially more intrusive. Want the names, addresses of people taking Prozac for depression? No problem. Computer users who like to gamble online? Who like sex toys? Bible believers and Hispanic political donors? It's all available to almost anyone who wants to pay. There's a good reason for these changes, apart from the fact that computers make the job much easier. Marketers dream of perfect lists, filled with names of rich, compliant, and acquisitive people. The quest is never-ending and, now, always accelerating.

For all the irritation they sometimes cause, these pitches spur millions of people to respond on a regular basis. At last count, such promotions generated $1 trillion in sales in 2003, almost double the sales a decade before.

The Trans Union people figured they could make more effective lists by relying on details at the core of their computer system: how much credit an individual had, the number of cards they had, whether they had any recent loans, and so on. The problem was, the Federal Trade Commission (FTC) considered the Trans Union lists the effective equivalent of a credit report. A 1970 law called the Fair Credit Reporting Act was enacted to protect individuals' credit reports from abuse. Though shaped by industry lobbyists, the law is a landmark of consumer protection in America. The commission told Trans Union in 1992 that it was breaking the law by selling its lists.

For years, the credit bureaus had been dogged by complaints. Information in their reports was chronically incorrect. They routinely failed to correct mistakes, and seemed arrogant when individuals called. Year after year, they were rated by the FTC as the number one target of consumer ire. Under pressure from the commission, the two other leading credit bureaus had stopped using credit information in their mailing lists. But not Trans Union.

In 1994, the agency formally brought an administrative proceeding to stop Trans Union from selling the lists. Trans Union fought hard. There was simply too much money to be made by these more refined lists. David Medine was in the center of the fight as the FTC's associate director for financial practices. He was intent on making use of the relatively few privacy laws to protect individuals. "It was a misuse of confidential information," Medine said at the time. "They were trading privacy for profits."

Medine described visits from Oscar Marquis, then Trans Union's general counsel. Medine understood clearly that, so long as Trans Union made more money selling credit information than they paid their lawyers, they would keep doing it, until a judge told them to stop. For his part, Marquis later said the company felt that it was entitled to continue, in part because it was providing a good service. He said the issue was not as cut and dried as the FTC lawyers argued. "We thought we were right and that the FTC was overreaching," said Marquis, now in private practice as a lawyer. "The definition of a consumer report is complex."

The case dragged on for years, with Trans Union appealing each ruling that they were violating the law. The company argued it had a First Amendment right to use information however it wanted. Ultimately, they tried to take their case to the U.S. Supreme Court. The Court's decision not to hear it out ended the case in June 2002. Now, it had to stop.

ONE SECRET TO ACXIOM'S SUCCESS is Charles Morgan's focus on business as an endurance test and his willingness to take risks. Acxiom is routinely cited by business magazines as one of the best places in America to work, in part because Morgan gives his employees, from senior staff to clerical workers, much latitude to manage. By all accounts, though, he expects them to be relentless about the company's basic mission: To find new ways to track, monitor, and profile people with data, and to find new ways to make money off of it.

Acxiom has all sorts of ways of providing these services, and it is instructive to read how the company itself describes what it does. "InfoBase Enhancement" enables Acxiom to take a single detail about a person and append, on behalf of its customers, a massive dossier. This generally happens without the individual ever knowing about it. Say someone gives a telephone number or address to a retailer. Acxiom can instantly attach details about their life, income, and family activities from the InfoBase list, the "industry-leading consumer data including demographics, home ownership characteristics, purchase behavior and lifestyle data."

The "dictionary file" of data contained in InfoBase Enhancement runs to eight pages. The document, shared with government officials after September 11, 2001, points to the many intimate details that fuel Acxiom's business. In addition to names, birth dates, genders, and addresses, it offers a wide variety of details designed to give database marketers precise glimpses at us and our families. This includes: number of adults, the presence of children, their genders and ages and school grades. It includes the home assessment, with ranges that go up by $50,000 and $100,000 leaps, the size in square feet, the market value. And it includes your occupation, net worth, estimated income, details about the credit cards you own. Another product known as Personicx takes stock of households according to income, spending habits, car ownership, and the like. In some ways, it replicates the sizing up that a neighbor might do of another neighbor, except for the fact that it automatically rates every household in America and few of them understand they're being judged. Acxiom calls Personicx "consumer segmentation," using the dispassionate language created by marketers.

One of the most compelling of Acxiom's products is the InfoBase TeleSource. When someone makes a toll-free call to a client of Acxiom to inquire about clothing or to buy some shoes, information about who the caller is and where he or she lives pops up on a screen in front of the telemarketer, even before the customer service representatives answer the call. Using TeleSource, the agent can often find out the kind of home the caller lives in, the type of cars the people in that household drive, whether they exercise. That's because the Acxiom service has amassed 160 million consumer telephone numbers, including up to 30 million that are unlisted, to help identify and profile people who call toll-free lines to shop or make an inquiry.

In the 1990s, the number of consumer calls to toll-free numbers operated by retailers and many others nearly tripled, to an estimated 24 billion a year. By 2004, the number of calls in to telemarketing centers eclipsed the number out to prospects' homes. One consequence: telephone numbers, even many that individuals pay to keep unlisted, are fast becoming consumer tags, identifiers akin to household Social Security numbers.

Acxiom officials said most of the information about the 160 million consumer phone numbers is gleaned from telephone companies' white pages and directory service files, as well as other public sources that fuel the company's giant computer system. Acxiom gets those numbers electronically or it buys the phone books and sends them abroad, where workers key them into computers. Company officials won't detail exactly how they gather the unlisted numbers, which they said represent about half of all unlisted numbers in the nation. They acknowledged that some of the information comes from "self-reported sources." Industry specialists said that could include surveys, product registration cards, and credit card applications. The company also gathers numbers from public records such as property data.

There are no laws prohibiting the collection of unlisted telephone information, according to officials at the Federal Trade Commission and the Federal Communications Commission (FCC). But Acxiom officials claim they follow limitations recommended by the direct marketing industry and are respectful of consumer privacy. Acxiom claims it won't give out unlisted telephone numbers willy-nilly; the company doesn't give out information about those numbers unless an individual calls a telemarketer.

Like others in the industry, Acxiom believes consumers grant permission to gather and use information about them when they make toll-free calls and engage company agents, regardless of the fact that almost no one knows that he or she has made such a bargain, or what it might entail. Telemarketers use phone numbers and associated personal details to provide personalized services, to tailor promotions, and to instantly distinguish profitable prospects or loyal customers from those seeking bargains. Marketers also use the phone numbers, and the information that can be appended, to improve customer service and prevent fraudulent transactions. "It's the difference, perhaps, between hunting with a shotgun and hunting with a rifle," Rick Ferry, executive vice president for the Miami-based Precision Response Corp., said about the growing power to monitor and target certain callers for pitches.

But many callers have no idea how information about them is being gathered and used. Even if someone wanted to block the identification of his home phone number, he can't because the owner of a toll-free number has a right to know who is calling for billing purposes. It's unclear whether any other company has as extensive a collection of unlisted numbers as Acxiom. But other information companies aggressively collect and use telephone numbers and data about callers. Targus Information Corp. provided a service called PhoneData Express, with the help of Acxiom, which the company says "allows you to append current name, address and other information to virtually every [U.S.] telephone number."

In the late 1990s retailers, cataloguers, and other companies on their own became adept in their use of toll-free lines and customer telephone numbers. Drug companies, for example, use toll-free numbers to attract patients and build databases. In one campaign, Merck & Co. worked with football coach Dan Reeves to promote a booklet about heart disease. When individuals called to get the booklet, they were asked their names, addresses, and a series of questions about age, health history, insurance coverage, and smoking and exercise habits—all of which went into a database. The industry has come up with its own rules governing the exchange of data. Acxiom won't share information until a "relationship" has been initiated between a caller and a company. When Acxiom appends personal information to a telephone number, most details generally do not appear on an agent's screen. Instead, the details prompt a computer to generate tailored scripts to guide the agent. Most people still assume that a telephone call remains a simple, ephemeral transaction. Fordham University law professor Joel Reidenberg, author of several books about information privacy, believes marketers are using telephone numbers as a proxy for Social Security numbers, which a growing number of people refuse to share because of concerns about privacy. "They can't go and ask you for your Social Security number," he said. "Instead, they're secretly taking your phone number and tagging your phone number."

Industry officials reject the notion that personal information is being collected surreptitiously, or that they're acting against the interests of their customers. But they acknowledge the industry's reluctance to highlight its growing technological prowess. Faced with the choice of unnerving callers by demonstrating how much they know, or discreetly using the information to direct a conversation, telephone agents generally opt for the latter course. That's why the agents rarely greet callers by name at first. "It gets people, including me, very nervous," said Gordon McKenna, president of the American Teleservices Association, an industry group, and chairman of TeleQuest Teleservices.

Acxiom underscores the growing sophistication of its services in literature about the InfoBase Profiler, which can instantly provide call centers with a caller's name, personal details, and household data, "and is entirely transparent to the consumer."

Allen Hile, assistant director in the FTC's division of marketing practices, believed this convergence will continue to dazzle consumers. But he cautioned that it may also expose them to scrutiny they don't understand or want. "It has just gotten so hyped up because computers are so much more powerful and databases are so much more accessible," Hile said in 1999. "Nobody is disclosing 'Hey, we're collecting your info.' Nobody knows."

• • •

ACXIOM AND OTHERS in its industry don't hide their sources. They just have never made much of an effort to disclose them in a way that most of us can understand. In financial documents on file with the federal Securities and Exchange Commission (SEC), Acxiom cites examples in the broadest possible sense: telephone directories, voter registration forms, tax assessor offices, questionnaires, warranty cards, catalogue buyer behavior information, and product registration forms. "Advances in computer and software technology have also unlocked vast amounts of customer data which historically was inaccessible, further increasing the amount of existing data to manage and analyze," says the company's annual report for 2003.

One Acxiom executive estimated that the number of warranty cards collected each year more than doubled from the mid-1980s, to 30 million by 2004. The warranty information, collected from 150 different manufacturers, represents about a third of all the households in the United States. In the mid-1970s, Congress approved a law requiring companies to automatically provide warranties. But people still believe they must always fill out the cards. In 1998, there appeared in magazines across the country a survey for a new marketing initiative. The survey asked readers to answer scores of questions about themselves by filling in many of more than seven hundred boxes. Do you suffer from depression or infertility? Experience stress or menstrual pain? What about gastritis and nail fungus? As much as this might sound like a medical form, it was actually a data collection effort by Condé Nast Publications, publisher of *The New Yorker, Vanity Fair, Vogue,* and more than a dozen other upscale magazines. It seems Condé Nast wanted to know its subscribers better. Much better.

The effort was designed to fill a data warehouse, with technical help from Acxiom. It asked for particulars about smoking, drinking (including "brands of spirits"), hobbies (collecting art or antiques, investing, and so forth), and shopping (at Bloomingdale's and other stores). It asked subscribers for the make, model, and year of their cars, the kinds of computers they own, and details about how they cruise the Internet. And it probed subscribers' intentions with regard to marriage, having a baby, and becoming a grandparent. Those getting married were urged to say when ("Please write in month, date and year in numeric format"). On page 5, readers found questions about twenty-five health-related matters, everything from "Acne/skin problems" to "Vaginal/yeast infection," all in alphabetical order. Also included are queries about drugs. "For which conditions do you or someone else in your household take prescribed medication?"

"What do you like? What do you want? Your answers to the questions that follow will allow us to target areas which interest you most and help us be most rewarding to you," says the introduction to the Preferred Subscriber Network survey. "Just answer the questions below to start the conversation and become part of this select group of subscribers to whom marketers listen first."

The survey intentionally sidestepped disconcerting questions about one's financial matters. That's because Condé Nast, like most other companies, could easily buy such data from information services like Acxiom to add to the details it gets directly from subscribers. The success of the publisher's data-warehousing effort over the next three years highlighted one ugly truth about the roiling privacy debate at the time. Even as people fret about corporate intrusiveness, they often willingly, even eagerly, part with intimate details about their lives.

Surveys are far from perfect. Some people lie. But data services like Acxiom and other marketers still rely on the answers as a rich resource. Besides, a startling proportion of people fill out questionnaires honestly, in part because they want to tell somebody about themselves. The impulse is approximately the same as when a guy starts talking about his divorce to a stranger on a crowded plane. It's worth noting that hundreds of thousands of subscribers filled in the eight-page booklets after they went out with magazines beginning in May 1998. What few of them realize is how their responses become part of a vast and growing information market.

"It's amazing. It's impotence and incontinence and all kinds of things they don't tell anybody," said Edward Nash, a marketing consultant and author of *Database Marketing: The Ultimate Marketing Tool*. "People tell us all kinds of things they wouldn't tell their neighbors.

"It's a release. Sometimes they want to let something out," said Nash, adding that surveys sometimes also make people feel like they're a part of something interesting. In some cases, they simply want to get something in return from companies they have faith in.

The Condé Nast program encouraged a sense of intimacy. In a "Dear New Yorker Subscriber" letter, publisher Thomas A. Florio said readers who responded to the survey would be those "to whom we can turn first for a valued opinion about the products you see on our pages or for a first look when there is something sensational looming on the horizon."

The company's Preferred Subscriber Network uses the responses in a program that connects readers and advertisers, including retailers, travel firms, and cosmetic companies, as well as drug manufacturers that want to market directly to patients with particular ailments. An organizer of the initiative said readers will appreciate tailored promotions. "What we're trying to do is enhance the relationship between the subscriber and their magazine," said the organizer, Stephen Jacoby, Condé Nast's vice president for marketing and databases. "In a sense, it's a benefit to the subscriber."

OTHER EFFORTS ARE STEALTHIER about their aims. A survey from General Electric asked shareholders of GE Investments for thoughts about the company's service, the quality of its products, and ways to improve. There was no place to put a name. What the survey failed to mention to the fifteen thousand recipients—most of them employees of General Electric Company, the giant parent firm—was that officials would quickly find out who filled in the circles indicating "Unacceptable," "Average," and "Outstanding." That's because the company included a code on the return envelope that corresponded with information in the company's shareholder database, allowing the company to surreptitiously identify every respondent.

A GE Investments official raved about the technique in a letter to the printer that helped devise the method. "This was, on the surface, a simple task requiring printing and collating various pieces for each shareholder's use. However, the hard part came with our request to be able to 'secretly' identify each respondent in the most discreet way," his letter to Harty Press of New Haven, Connecticut, stated.

"I must especially compliment one of your employees. . . . Her suggestion enabled us to secrete the code in a manner least likely to attract attention from the respondents," the official went on. "She's terrific!"

Such ploys have been used for years by some market researchers, who pine for personal information about individuals but know that respondents sometimes grow shy when they must include their name on a survey. But the methods have become far smoother in recent years, as computer technology makes it easier than ever before to link coupons, surveys, or other materials to databases of information about individuals.

The mechanism might be a bar code. It might be a cluster of dots. In the case of GE Investments' survey, the identifying information was contained in a series of numbers.

GE Investments is a money management arm of General Electric that oversees about $80 billion in assets for individual and institutional investors. The survey went out to shareholders of the company's mutual funds. It was intended to help the company improve service and identify the particular concerns of individual investors. Tim Benedict, spokesman for the company, noted that it did not explicitly say the answers would be confidential. Benedict said it was the first—and last—time the company used such a code. "We basically didn't ask for the customer's name and address because we wanted to encourage a response." And Benedict added: "We wanted to know who was answering. . . . It was not to pull a fast one on our customers."

That wasn't good enough for GE chief executive Jack Welch. In an extraordinary mea culpa, he sent an email message to several hundred thousand employees condemning the coded survey, saying it was "clearly wrong and should never be repeated."

CHARLES MORGAN NEVER MUCH CARED about working with the government. The red tape was too cumbersome and the profits too low, in part because the government didn't seem technology savvy enough to make full use of Acxiom'sophisticated systems. The September 11 attacks abruptly changed the equation for him. Morgan and his colleagues reached out to many of their contacts in the government and in politics. One of them was Bill Clinton.

When the planes crashed into the World Trade Center and the Pentagon, Clinton was in Australia with his daughter Chelsea. It was a serious situation, given that no one knew whether the United States was in the first stage of a war. The Bush administration, forgetting its fierce political differences, sent a plane to pick up the former president. A few days later, he was sitting in his den in the Chappaqua, New York, house when Paul Leopoulos called. Leopoulos, one of his closest childhood friends from Arkansas, worked as a sales and training executive at Acxiom.

Leopoulos told Clinton: You've got to see what we have here. We have information on a number of the terrorists. Maybe we can stop future attacks. We can help find these guys.

Based on a few scraps of information in newspapers after the attacks, Acxiom queried its data and found names, addresses, links among the terrorists, and telltale inconsistencies. The data showed the attackers had used invalid driver's licenses and phony telephone numbers. "We were trying to figure out where these guys had lived and we were trying to figure out everything from improper use of credit cards and who they might have been associated with," Morgan said two years later.

It didn't take much to convince the former president. Acxiom was no stranger. Morgan and his crew at the company were supporters of Clinton and Hillary, donating money to their campaigns and rallying on their behalf in the state. Clinton picked up the telephone and called one of his most ardent political foes, Attorney General John Ashcroft. He urged Ashcroft to give Acxiom a hearing, and Ashcroft agreed.

Not too much later, Clinton visited Morgan's office in a new building overlooking the Arkansas River. He was guarded by a team of Secret Service agents. Morgan and Clinton sat side by side as Morgan showed what Acxiom had. "He was just sitting in my little bitty office," Morgan said. "He caught the significance of a lot of things almost before you say them." The episode was a turning point of sorts in Acxiom's history. Suddenly a new market, based on the fear of terrorism, had opened.

Morgan suggested the change grew out of a sense of civic responsibility. Acxiom, he said, was obligated to use its data and privacy smarts on behalf of the government. It knew the people, had their names, addresses, and all the rest, and could say whether they were who they claimed to be. It could monitor credit activity and track people to a large degree through their purchasing behavior. "Activities in and around 9/11 caused us to rethink that and we developed a sense among the leadership at Acxiom that for this country to be a safer place they had to be able to work with information better," Morgan said in November 2003, after refusing for nine months to discuss the company's homeland security efforts.

"And 9/11 showed us that the U.S. government and its information processing capabilities were at the level we were at in 1973. And that it—if we were going to have a safe country the government was going to have to do a lot of upgrading and investing. And we also knew that would have to be done in an environment where privacy and data use and practices have got to be carefully thought out so that we don't create the fear, doubt and concern of Big Brother. Big government, Big Brother. We thought we could help work on that balance."

In other words, the company decided to become a major player in the war on terror, to use its reservoirs of personal information in a new way.

THE FLETCHER ROOM was a space deemed by bureaucrats at the Department of Transportation to be among the ugliest in all of Washington. It had no windows, ancient chairs in frayed maroon polyester cloth, walls covered in dingy cream fabric. Into this drab scene walked retired Army General Wesley K. Clark, a West Point graduate and Rhodes Scholar who was contemplating a run for the presidency. Clark carried great prestige, having served as Supreme Allied Commander in Europe. When he retired in 2000, Clark was awarded the Presidential Medal of Freedom, the nation's highest civilian honor.

On that day in December 2001, he was an Acxiom man. An Arkansan, Clark had recently joined Acxiom's board of directors. At the same time, he worked as a hired hand, using his prestige and connections to open doors for the data giant. He appeared impressive as he described the company's audacious plan to team up with another little known company, HNC Software, to create a massive passenger profiling system. At the core of Acxiom's effort would be a program called AbiliTec, which uses a 16-digit number as a stand-in for names, an approach that dramatically accelerates the processing speed.

The system Clark described to transportation officials would combine personal data along with information about the reservations and seating records of every U.S. airline passenger. Acxiom was offering only a subset of the information it manages. Under contracts with other data providers, Acxiom cannot share some information gathered for marketing purposes. What Clark was suggesting, however, would more than do the trick to clearly identify people and, if necessary, their associates. In a matter of seconds, HNC software would take the information and, using software that can learn from massive amounts of information, examine it for subtle signs of deceit or malicious intent. It would authenticate the identity of every passenger.

Government authorities would then use artificial intelligence and other sophisticated software, along with behavior models developed by intelligence agencies, to determine whether the passenger was "rooted in the community"—whether he or she was well established in the United States—and find links to others who might be terrorists. According to a secret government document, it was to be an "automated system capable of integrating and simultaneously analyzing numerous databases from Government, industry and the private sector . . . which establishes a threat risk assessment on every air carrier passenger, airport and flight."

Clark was well paid for his presentation and for his efforts in general on behalf of Acxiom. In 2002 and 2003, he received nearly half a million dollars. Before the announcement of his presidential candidacy in September 2003, he received an annual $150,000 retainer plus commission "for new business." Acxiom got what it paid for: access. Even as he took care to keep a low public profile, Clark worked assiduously on Acxiom's behalf to open doors in Washington. He arranged meetings with FinCEN, the Treasury office that collects and data-mines suspicious activity reports from financial institutions. He took the company into the intelligence agencies. He sat in on an intimate session with Vice President Dick Cheney in the vice president's office in the Senate. Early in 2002, Clark approached a new operation at the Defense Department called the Office of Information Awareness. Run by former Vice Admiral John Poindexter, who had been Ronald Reagan's national security adviser, the office aimed to create unimaginably large data systems and surveillance networks. The system Poindexter envisioned would be larger and more powerful than even the global eavesdropping technology run by the supersecret National Security Agency

(NSA). Poindexter and his colleagues were impressed by Acxiom, according to internal email.

Joining Clark as Acxiom lobbyists were other well-connected Arkansans, including former Transportation Secretary Rodney Slater and former Arkansas senator Dale Bumpers, who had benefited from Acxiom's fund-raising prowess so many years before. Former Clinton chief of staff Thomas F. (Mack) McLarty III, who also sat as a director on Acxiom's board, received consulting fees of about $175,000 annually, through a company he runs called McLarty Management Company.

Acxiom was like other information services on the make—indeed, high-technology companies of all kinds. The company used people like Clark, Clinton, and other representatives to transform its own image. Suddenly Acxiom was also an anti-terrorism company. Not only could it better target people for marketing and weed out fraud for businesspeople. Morgan's staff told the government it could now authenticate people and truth-squad the information they shared about themselves.

MAGICIAN DAVID HARRIS stood beneath a large silver globe, barking out his pitch from the Acxiom booth on the floor of the Jacob Javits Convention Center in New York. The occasion was the Direct Marketing Conference of June 2003, a glitzy affair that gives data-driven firms a chance to sell their services to one another. "Ten seconds," he boomed. "Watch one trick!"

As people gathered around, Harris handed out three worn paperback books, including Dale Carnegie's *How to Stop Worrying and Start Living.* He told the crowd he was going to read their minds, and he focused on one woman holding John Grisham's *The Client* open in her hands. She looked back and forth from the book to Harris's face. "I see an 'e' toward the end of your word. It's not the last letter. It's the second to the last letter, and the last letter is 'r,'" Harris said. He tilted his head, leaned forward, and pointed to the woman. She mumbled her assent. He asked her a few more questions, then declared the word she was looking at was "photographer." He was right.

As the hired entertainment, his job was to convince visitors at the conference that his parlor tricks added up to real magic. He drew them in, dazzled them with his show, and then let the Acxiom sales team, including a guy named Rob, do its thing. Harris, who made his living as a "hired gun" working at conventions for a wide array of companies, salted his patter with words like "content" and "data." "Rob and I can tell you in forty-five seconds what we do," he boasted at the conference. "We help manage, grow, and keep customers."

On cue, Rob the salesman jumped in with his own patter. "We are a one-stop solution," he told the crowd, noting that the company's latest product had information on almost 200 million people living in 110 million households. "What we do is no illusion. It's straight up."

Acxiom officials convey the same message about personal privacy: We're straight up. In promotional material and on Capitol Hill, the officials portrayed themselves as working in the best interest of consumers. At the same time, the company also lobbied hard against legislation that might curtail its access to personal information. Over and over, company officials worked with lawmakers to fashion rules that preempted tougher state laws. (One of their arguments: that a variety of strict state laws might confuse people.) They claimed to support what is known as fair information practices, but they resisted following some of the basic tenets. They talked about how everything would cost more if Acxiom and its competitors lost access to information about you. The economy would suffer.

Acxiom knew that concerns about privacy, were they to become acute enough, could lead to legislative and regulatory reforms. Almost $1 billion in revenues was at stake. At the same time, the company knew perfectly well that its business would be considered massively intrusive by many people—at least for many of those who understood that business. Former spokeswoman Marice Gardner once made a joke about it: "My mom says I work for Big Brother."

The company was relatively lucky. It had managed to stay off the radar screen of regular Americans, even as it promoted itself aggressively to major financial institutions, direct marketers, insurers, retailers, and the like. Regular people seemed more worried about the impact of the World Wide Web.

JENNIFER BARRETT WALKED into a sparsely furnished office high up in Acxiom's new $50 million administrative building, a handsome facility that overlooks the muddy Arkansas River and a highway heading in the direction of Texarkana. Not far upriver was the Clinton Presidential Library, still under construction.

Barrett has a computer science background, and in the early days when Acxiom was still called Demographics, she wrote code. She has worked as a product developer and, in recent years, as the company's "privacy officer." Her job involves serving as an internal watchdog and the face and voice of Acxiom, particularly during policy discussions about laws and regulations that might curb the company's access to personal information.

Barrett has red hair and deep brown eyes that can sparkle one moment and grow wary the next. She laughs easily, giving the impression of spontaneity, but she also relies heavily on pat phrases and arguments of the sort she uses frequently in congressional testimony and policy papers. Like any good marketer, she rarely strays from the pitch she is making. To her way of thinking, Acxiom serves as a trusted third party that oversees personal information. And the company helps provide individuals with more shopping opportunities, quicker loan approvals, targeted marketing promotions, and an array of conveniences. She believes that most people don't know or care how their information is used to generate these Information Age benefits, as long as they keep coming. "They love it. They don't have any idea why they get it. There's a total disconnect," she said. "I have a personal belief that the consumer doesn't really want to know."

Barrett underscored her idea by pointing to the light switch on the wall. She compared the flow of names, financial records, spending habits—and the many other digital details that comprise our lives—to the flow of electricity that keeps the lights on. "I don't care to know how the electricity gets to that light switch over on the wall. But when I punch that light switch, I want the lights in this room to come on and I want them to come on pretty quick, okay?

"The value the information brings to the consumer is a little bit like that. We're living in a very information-, infrastructure-rich society today. It used to be, you know, technology and electricity and all the things that we went through in the industrial revolution. And now that we're in an information revolution—or whatever you want to call it—information has become the grease that gets things done faster, quicker. You know, it makes the engine run. And without it, things slow down. We're a very time-sensitive society."

This is Barrett's buildup to her core message, the one Acxiom has used so effectively over the years in Congress. Don't regulate information services heavily—or else risk losing all the Information Age benefits we have come to expect. "Politicians in general—there are always exceptions—are beginning to recognize that writing good information management law is very tricky," she said. "And you do not want it to be driven by anecdotes or incidents. You really want to understand. I mean, we don't outlaw knives, even though people are stabbed to death."

THAT'S BARRETT'S JOB, to make that kind of argument. She does it well, both for Acxiom and the industry in general. Despite her title as privacy officer, and the claims the company makes as a leader of privacy policy in America, Barrett's role often is to fend off anything that might constrain Acxiom from gathering and using whatever it can to bolster the company's bottom line. It's a brash approach, to say the least, and very effective.

In March 2002, as the company was pressing hard to win contracts to provide data to the government for screening and surveillance initiatives, Barrett and Morgan teamed up on writing a briefing paper on privacy. In a magazine-style brochure called *Beyond Consumer Privacy to Consumer Advocacy*, they argued, somewhat paradoxically, that the more information that flows to Acxiom and its clients, the more privacy individuals will have. More important, they wrote that there would be huge economic costs if the flow of data to marketers and companies like Acxiom were slowed.

"There's no question that protecting consumer privacy is important and should be done," their paper about consumer privacy stated. "At the same time, we cannot ignore the fact that the free flow of information has a positive impact on consumers' pocketbooks. So are privacy and responsible data usage somehow mutually exclusive? Absolutely not."

Morgan and Barrett used their briefing paper to tout AbiliTec, which Acxiom claimed could dramatically improve a client's ability to draw together information about a particular customer. The executives said AbiliTec could help a company "move from being merely concerned about consumer privacy to becoming an aggressive consumer advocate."

By the spring of 2003, though, their claims for AbiliTec had evolved. Now the technology was also being packaged and sold as a risk management and screening tool for the government's war on terror. "We also believe that in the post–September 11 environment, certain governmental agencies have a need for the type of data integration solutions enabled by AbiliTec," the company wrote in its annual report. "Since September 11, 2001, we have been actively pursuing government contract work in this regard."

Barrett has spoken to Congress about privacy on a number of occasions. In a September 2002 appearance before the House Subcommittee on Commerce, Trade and Consumer Protection, she represented Acxiom; Experian Marketing Service, an arm of the giant credit bureau formerly known as TRW; and Trilegiant Corporation, one of the nation's largest direct mailers. At issue was legislation that might limit the kinds of personal information direct marketers could gather. "Our clients represent a who's who of America's leading companies, and we are always proud of the reputation for helping them sell better products, smarter, faster, and at a lower cost," Barrett began.

Her main goal that day was to ensure that legislation under consideration would not require companies to say how they are collecting and using personal information, or give individuals a chance to say no. She opposed rules or laws that would put oversight of company activity in the hands of the government. She also wanted the committee to be sure to prevent states from writing tougher consumer protection laws, saying in effect that that wouldn't be fair to consumers. "Nothing will be more confusing to consumers than to have differing privacy laws in each state or locality," she said.

Implicit was the idea that a variety of state laws would cost Acxiom and its clients a lot of money and, perhaps, cut back on its access to information about people. But she never said this outright in her testimony.

Barrett applauded the panel's plan to limit the ability of individuals to seek access to the files companies maintain about them. Providing that kind of access is a part of the fair information practices Acxiom professes to support: proper notice to individuals about what is being collected about them, the individual's choice not to participate, and the ability to access any information that's being collected to ensure it's accurate. But it also is inconvenient for the company and costs money to provide.

As she spoke to Congress, Barrett pulled off the trick of seeming to support these fair information principles while in fact opposing their spirit almost head-on when they cut too close to Acxiom's business. Or at least trying to bend them in Acxiom's direction. "Each of the four fair information practices principles—notice, choice, access and security—must be applied uniquely to strike a balance between the value gained by the consumers, business and society and the associated cost," she said. "The primary purpose of access is to assure that information a company maintains about an individual is accurate.

"However," she added, "access for the sake of curiosity is never justified." Her courting ways worked, and she continued in her unusual role as the company campaigned for government business, much of it cloaked in secrecy. In 2002, Barrett counseled a senior counterterrorism official in the Transportation Security Administration (TSA) on how to handle questions about privacy at a public forum. John Poindexter's Information Awareness Office was also smitten with her reputation on privacy. "Acxiom is the nation's largest commercial data warehouse company. . . . They have a history of treating privacy issues fairly and they don't advertise at all," one official said in an email to Poindexter. "As a result, they haven't been hurt as much as ChoicePoint, Seisint, etc by privacy concerns and press inquiries. . . . Ultimately, the U.S. may need huge databases of commercial transactions that cover the world or certain areas outside the U.S.," the official wrote. "Acxiom could build this mega-scale database."

In order to avoid panicking people, Acxiom officially suggests a different approach: Don't build one giant database. That's bad for public relations. Use networks to link those data systems together.

BARRETT HAS LONG INSISTED that regular people don't care as much about data collection and privacy as they sometimes claim. "It's not about the collection, it's all about the use," she liked to say, echoing the gist of her message to regulators over the years. "I think the consumer is saying, 'I want the information about me to be under control, not necessarily under my control.'"

But a series of privacy storms in the late 1990s and early 2000s showed that privacy had become an incendiary issue and frequently riles both liberals and conservatives.

In 1998, a company called Image Data sparked a national debate by quietly buying state driver records, including driver photos. Officials from Image Data portrayed themselves as working in the public interest. The company said it intended to build a national database of photos and personal information to help retailers prevent identity theft, an epidemic crime in which fraud artists use victims' personal information to run up bills in their names or empty their bank accounts. Company officials claimed the service could head off billions of dollars in fraud by giving clerks an instant, tamperproof way to verify the identity of customers.

Like Acxiom and others, Image Data was taking advantage of cheaper data storage and networks to devise a completely new service. It appeared promising. Image Data bought the photographs for less than a penny each. Those images were to be cross-referenced to personal information gleaned from public and private sources. In addition to a name and address, the company's databases held an individual's Social Security number, age, sex, race, and other details from a driver's file, as well as limited information about each transaction. Image Data's plans called for a national database to come into play whenever a customer at a participating retailer attempted to use a credit card or check. Identifying data was sent to Image Data computers, which would respond by sending a photo back to a small screen mounted discreetly near a cash register. The transaction would proceed only after a clerk verified the customer's identity.

The company's desire for motor vehicle files was far from novel. Acxiom, for example, depends heavily on such files to locate and describe people. These records were routinely sold by many states and had become a computerized staple for direct marketers, information services, and others. But by adding photographs into the mix, Image Data had crossed into new territory, raising on the one hand the possibility of improved security for consumers and retailers and, on the other, new questions about personal privacy.

The service was part of a growing number of surveillance and identification systems that take advantage of computers, electronic networks, personal information, video images, fingerprints, and other identifying data, generally in the quest for security. Law enforcement authorities now use computer-assisted cameras to "read" license plates of cars that have run through red lights. Casinos use such cameras to watch for the faces of con artists or card sharps in their digital picture files, and police in Britain are using them extensively in public areas to automatically scan for known criminal suspects. Some automated teller machines now require users to offer a finger for scanning rather than a bank card to get access. And growing numbers of banks, including First Union, require some people to provide a thumbprint before cashing their checks.

Privacy activists said they feared that once photos are released by authorities in digital form, they will be used for other purposes by private detectives or telemarketers who want to match a face to other personal information. "It contributes to an atmosphere where people feel they are being watched," Robert Smith, publisher of *Privacy Journal* newsletter, said at the time. "What you create is a mug file of law-abiding citizens."

Image Data downplayed the concerns. Company officials said they only wanted to stop fraud. "What we're looking for is security of the entire process," Image Data spokeswoman Lorna Christie stressed. "This is a great example of how technology can be used to protect citizens and business."

It turns out that in 1998 Image Data had quietly accepted nearly $1.5 million in federal funds and technical assistance from the U.S. Secret Service. Congressional leaders who helped make those arrangements envisioned using the photo file to combat terrorism, immigration abuses, and other identity crimes—applications that appear to go beyond company claims the database would only be used to prevent check and credit card fraud.

"The TrueID technology has widespread potential to reduce crime in the credit and checking fields, in airports to reduce the chances of terrorism, and in immigration and naturalization to verify proper identity," stated a letter about Image Data LLC from eight members of Congress in September 1997. "The Secret Service can provide technical assistance and assess the effectiveness of this new technology." Thousands of people in South Carolina, Florida, and Colorado complained they were never told their images, at least 22 million of them, could be sold. As the company lobbied to gain access to motor vehicle files, officials apparently told few people about its ties to the Secret Service or the money it received from Congress.

With help from an influential Boston public relations firm, the Rasky/Baerlein Group, Image Data hired lobbyists in Florida and South Carolina. The company spent about $25,000 on the South Carolina lobbyist—five times the cost of the database it eventually bought. It contributed $500 to state Senator John Land, the legislator who sponsored a bill enabling the sale, as well as $1,000 to former Governor David Beasley. Image Data also received help from eight legislators on Capitol Hill. They include Senator Judd Gregg (R-N.H.), who received $2,000 in campaign contributions in his last campaign from the company's officials or their families, and Representative Charles F. Bass (R-N.H.), who received $3,000 in contributions from company officials since 1995, according to Federal Election Commission data.

State legislators, motor vehicle administrators, and others who worked with the company said they had no inkling that federal officials might be involved. When the arrangement became public, people went nuts. Several officials from Florida and South Carolina said they felt misled by the company. Florida governor Jeb Bush canceled a contract to sell 14 million photographs. Colorado governor Bill Owens halted the sale of 5 million images, while the state legislature pushed through a bill that would ban the transfer. South Carolina attorney general Charles M. Condon sued the company for the return of 3.5 million digital photographs already being used in a pilot project there. State legislators, meanwhile, proposed laws blocking future sales and a South Carolina woman filed a class-action lawsuit on behalf of others seeking to stop Image Data from using the images. Officials in Florida, Colorado, and New York have said they intend to study sales of personal information by their states, with an eye toward new restrictions. Congress requires states to change the rules on the sale of such records, or risk losing transportation funds.

Robert Houvener, the founder of Image Data, portrayed himself and his colleagues, some of them veterans of the direct marketing world, as well-meaning corporate newcomers overwhelmed by attention from the

media and policymakers. "We've been forthright with everyone," Houvener said. "There's nothing inconsistent here at all."

THEY GATHERED IN LITTLE ROCK, chief executives and privacy officers from Internet, marketing, medical, and banking companies, all there at the request of Charles Morgan and Jennifer Barrett. The idea was to talk about pending battles with regulators, Congress, and activists over how to properly harvest and use the many details about individuals' lives. Though the September 11 terror attacks were still a year away, the meeting offers insight into how Morgan and his colleagues think about their place in the world.

The group Morgan had assembled was intimately aware of a series of intense controversies that had made privacy a touchy national issue. In addition to Image Data, a national uproar over medical records had been caused by a small Massachusetts company called Elensys. It seems that with no public discussion, Elensys had made arrangements to collect prescription records from pharmacies and, on behalf of particular drug companies, to send out "educational materials" reminding patients to take their medicines. Problem was, they never asked the patients for permission. The ensuing outrage prompted CVS and Giant pharmacies to back away from Elensys and buy full-page newspaper advertisements to apologize to customers.

Before that, Intel withdrew plans to include a unique identifier on every processor it produced, after computer users howled with indignation. The online advertising giant DoubleClick had been hammered for its plan to combine online browsing habits with offline shopping records compiled by a data cooperative called Abacus, a company allied with Acxiom. There were plenty of other examples. The government created its own stink with Know Your Customer, a proposal to require financial institutions to monitor customers more closely for signs of money laundering. That plan was loathed and blasted by conservatives and liberals alike, leading the government to abandon the plan.

On the day of Morgan's roundtable meeting in Little Rock, financial services companies were facing a costly and cumbersome federal requirement to provide privacy notices that, for the first time, would disclose how they collect, sell, and use customer records. Americans, including Congress, were beginning to understand. They were being watched, analyzed, tracked like never before. They loved the Internet and thought it was nifty when companies seemed to know them better. But they wanted some control over their own information.

Morgan set the tone with his remarks. The transcript of the meeting shows he was intent on selling a vision in which companies like his maintain responsibility for policing themselves. He was all for privacy—as long as it didn't hurt his business.

He clearly didn't believe Congress was up to the task of striking that balance. "My observation in general is that industry is moving as quickly as possible to address a lot of these issues and even what I would call opportunities that are offered by the better use of information," Morgan said. "Also, my further observation is most of these companies are acting in a very responsible manner vis-à-vis privacy. They want to do the right thing. They really don't want to invade people's privacy.

"But my big concern right now is that legislation or regulation is potentially actually going to get in the way of all this happening. And, obviously, it's going to impact the potential success of companies, as laws are passed that restrict the flow of information.

"What is particularly alarming to me is that the guys who are framing these issues—the lawmakers who are casting votes on Capitol Hill—are not really wired into these issues."

Morgan used a colorful analogy that he believes lawmakers and others should consider before imposing restrictions on his industry—the same analogy Barrett used with me three years later.

"There's a very large inherent risk in having a 70-mile-an-hour speed limit on the Interstate," he stated, "because we know that about 40,000 or 50,000 people die in automobile accidents each year. But we've decided that 70 miles an hour and 41,000 deaths are an acceptable risk and return.

"If we legislate a five-mile-an-hour speed limit, 41,000 people would live next year. However, the lifestyle that we enjoy would be severely changed." Morgan told the group that "You can put sort of that same analogy in the flow of information. If you just totally stop it, we're going to suffer a lot."

• • •

AT THE END OF 2003, Acxiom began work on a fence around its Conway campus. The fence would keep unwanted visitors at a distance. The company had never had to think about such things before, since very few people had ever heard about it. That's changing as more and more people come to know Acxiom, not all of them friendly.

One of those curious people was a young Ohio man named Daniel Baas, a systems administrator for a data-mining company in Cincinnati called Market Intelligence Group. The Cincinnati company was hired by Acxiom to analyze some data. As a consequence, Baas had regular access to an important Acxiom computer server.

Baas is bright, somewhat nerdy, a hacker. He liked to explore computer systems, and got excited about finding gaps in security and exploiting them. That wasn't hard at Acxiom. During one of his electronic forays he discovered a file containing encrypted passwords for some of Acxiom's largest customers—banks, credit issuers, retailers, and other businesses who maintained billions of customer records there. Baas had hit paydirt. Using a widely available software program, he decrypted the passwords. He found one that opened all the files. Then he began downloading. Authorities say he took the names, credit card numbers, Social Security numbers, addresses, and other details about an estimated 20 million people. The information was burned on about thirty CDs.

The breach was grave, but far from uncommon. Like so many other companies and government agencies, Acxiom had failed adequately to secure the information it had collected. The company did not even detect the lapse. It was local sheriff's investigators who turned up Baas's name during the probe of another hacker in the area. The investigators found logs of online chats between that hacker and Baas. They later searched Baas's home and found the CDs containing the Acxiom data.

The case was turned over to federal prosecutors. In the summer of 2003, they said Baas "exceeded his authorized access" to a protected computer. In December of that year, Baas pleaded guilty to one count. Though Baas had offered to share the information, he never did.

Acxiom officials flew up to Cincinnati to talk with the hacker, who told them how he had entered their system and taken the information. They informed their clients about the breach. But they didn't bother to tell individuals their information had been stolen. A company official said the information was simply not that sensitive and "did not meet a threshold that would require customer notification."

They told prosecutors that the information Daniel Baas obtained had a market value of $1.9 million. They estimated it cost them $1.3 million for security audits and encryption software to fix the gaps he had exposed. It turns out that wasn't the only incident. When Acxiom examined its files, it found that other hackers from Boca Raton, Florida, had gained access for months—also by taking advantage of access through a business associate of Acxiom.

Security specialists shuddered at the episodes, not only because Baas got into the Acxiom system so easily but because the company did not feel obligated to reach out to the people whose names, addresses, and other personal details ended up on Baas's CDs. "Obviously, they should have protected the data better," said Kevin Poulsen, who wrote about the incident at SecurityFocus.com, a Web site devoted to such issues. "The fundamental problem is we have no rights to have our data protected, because it doesn't belong to us."

LONG AFTER the terror attacks, Charles Morgan had high hopes about the company's new ties to the government—and business in general. Morgan predicted that Acxiom and other information services were just beginning to learn how to exploit the oceans of data they had collected.

"The information is all there, but the ability to analyze it has really not been there on the grand scale until fairly recently," he said, charming but focused as ever as he steered his way through difficult issues about privacy and security. "We have built database marketing systems that are a snapshot in time, but in general we have a today snapshot in time. And what we are saying today is we are going to keep that snapshot and tomorrow's snapshot and next year's so that we have years of those historical snapshots that can go into the analytical process."

Morgan was asked whether people should trust Acxiom to do the right thing with those snapshots—the virtual dossiers they can pull together so quickly about almost anyone in the United States—for marketing or security.

"I think that regular Joes on the street pay little attention to Acxiom. But should we come to their attention, we need to make sure they feel there are the appropriate laws in place and that they are comfortable with our published information," Morgan said.

"And the average person probably doesn't care. But for those who do, they need to be able to find the information out that gives them the level of comfort that they need."