No Place to Hide

FREE PRESS
A Division of Simon & Schuster, Inc.
1230 Avenue of the Americas
New York, NY 10020

For information about special discounts for bulk purchases,
please contact Simon & Schuster Special Sales:
1-800-456-6798 or business@simonandschuster.com

Designed by Karolina Harris

Manufactured in the United States of America

3 5 7 9 10 8 6 4 2

Library of Congress Cataloging-in-Publication Data
O'Harrow, Robert
No place to hide / Robert O'Harrow, Jr.
p. cm.
Includes bibliographical references and index.
1. Information technology—Social aspects. 2. Information society. 3. Electronic surveillance. 4. Privacy, Right of. I. Title.
HM851.04 2005
303.48'33'0973—dc22 2004056397

ISBN 0-7432-5480-5

AUTHOR'S NOTE

No Place to Hide would have gone nowhere without the intellectual and financial support of the Center for Investigative Reporting. The center is a stronghold of journalistic idealism. It exemplifies Brandeis's idea that sunlight "is said to be the best of disinfectants" through its support of an array of muckraking projects. The center's financial backing gave me the time to figure out a direction for the book, write a proposal, and travel extensively for original reporting at the project's core. Some of that money came from philanthropic groups, including the Ford Foundation, the Deer Creek Foundation, and the Carnegie Corporation of New York.

As important as the money was the enthusiasm of the center's director, Burt Glass, who thrashed through ideas with me during innumerable phone calls. Burt never wasted a chance to express his confidence in our endeavor.

INTRODUCTION: NO PLACE TO HIDE

THE PENNSYLVANIA CONVENTION CENTER fills two long blocks in downtown Philadelphia. With more than 400,000 square feet of exhibition space, the main hall has enough room inside to hold a track meet, or six football fields, or some rather large parties. The center is known as the home of the city's annual flower and car shows. Organizations from around the country also gather there for the proximity to the city's historic sites: the nearby Liberty Bell, Independence Hall, and other landmarks from the nation's birth seem to convey a certain integrity to their activities. It's where the International Association of Chiefs of Police had its technology conference in October 2003.

For several days, thousands of law enforcement officials from the United States and abroad wandered through the exhibits. Some lingered at booths featuring dull black handguns. Others inspected a minitank designed for riots. They eyed crisp blue uniforms and tried on bulletproof vests. They formed a long line for the virtual shooting range, a training system that came complete with a life-sized culprit projected on a video screen. The *pop, pop, pop* of their practice sessions filled the air. But the great majority of police came to Philadelphia to

look at a different sort of gear. They wanted the stuff of homeland security: databases and dossiers, surveillance cameras, and computer tools for intelligence analysts. And in greater numbers than ever before, the information industry was there to oblige them.

The center was abuzz with an atmosphere that could be described as part carnival, part science fiction. Row after row of pitch men and women touted their companies' ability to preserve life and liberty by helping police watch everything more closely. One contractor, Raytheon Communications Infrared, displayed a car with a night-vision camera mounted on the roof. The FBI promoted its growing use of DNA to identify people, while Treasury agents touted their growing access to reports about suspicious bank accounts. PricewaterhouseCoopers, the accounting and consulting firm, was among those offering a slick handbook describing how best to seize computers, email, and telephone calls. There was even a group, partly funded by the Justice Department, giving away a CD showing local police how to become intelligence agencies, not just crime-busters. "Turn-Key Intelligence: Unlocking Your Agency's Intelligence Capabilities," the CD was labeled. "Today's emphasis on intelligence makes it a must-do for most agencies in the United States."

Near the entrance was information giant ChoicePoint, a Georgia company marketing its ability to deliver billions of records about Americans online to police in every state. Names, addresses, jobs, cars, family, criminal records. ChoicePoint collects, analyzes, and sells it all. Next to its booth were firms that help law enforcement manage the ChoicePoint files. One of them showed how it delivers the reports to cell phones, PalmPilots, and laptop computers. Another, Orion Scientific Systems, claimed to help police use the data to identify and track troublemakers who might be criminals or terrorists. "Orion develops and implements all-source automated collection and analytical tools designed for intelligence, law enforcement and global security analysis," the company's brochure said.

Not far away was a LexisNexis display. A salesman dressed in a golf shirt showed how the company's own collection of personal records, legal cases, and billions of news articles can help track someone down. "We have a lot of derogatory information on people. Judgments, liens, bankruptcies . . . ," the salesman said to a police chief from a little town in Kansas. Across the aisle was one of the LexisNexis partners, a technology company called I2, which does something called data mining. Data mining is a computer process that helps reduce the amount of time it takes to discover a nugget of information gold in a giant database from weeks or months to an instant or two. The I2 software spits out graphic displays about a person's activities and associates that look like colorful spiderwebs. The company's aim echoes the futuristic law enforcement world in the science fiction movie *Minority Report*, where one group of police specializes in rooting out actual crimes before they occur. "We are," said I2 president John J. Reis, "principally a company whose focus is all about converting large volumes of information into actionable intelligence, to help the law enforcement and intelligence communities resolve crimes faster and through predictive analysis help to thwart crimes before they occur."

There was a company called Identix whose salesman cheerfully demonstrated the workings of a small machine called IBIS. Though i looked like a handheld vacuum cleaner, it was actually an identity tool The IBIS had a small hole in the front to electronically capture finger prints. Above that was a dime-size lens that takes digital photos of suspect's face. The Identix salesman explained that the device wa meant to improve police efficiency by enabling them to wire the finge and face prints back to headquarters for verification. Identix also ma kets one of the nation's most sophisticated face recognition program

In the back of the great hall was Verint Systems, a company whos name is derived from "verifiable intelligence." Verint works closely wit marketers, who use the company's technology to track and assess cu tomers. But it was there to promote its catalogue of surveillance ge Verint had important contracts with the Defense and Justice depa ments, but it wanted to expand its market to state and local police. T company displayed eavesdropping equipment that could listen in telephone calls, capture email from the Web, and sift through digi video recordings for suspicious behavior.

Generating its own buzz was a firm called Seisint, short for seisn intelligence. Seisint's main product is Accurint, an information serv that holds out the promise of giving police entry into society's ev nook and cranny. "Instantly FIND people, their assets, their relativ their associates, and more," the marketing material said. "Search entire country for less than the cost of a phone call—a quarter."

What made Seisint stand out, though, was a new service called the Multi-state Anti-Terrorism Information Exchange. Whimsically dubbed the Matrix, in a nod to the popular dystopian movie, the system combines commercially available details about American adults with millions of criminal and government records. That had never been done before, at least not publicly. The company wasn't shy about what it could mean for regular cops. The "invisible become visible," its leaflets said. (Police who had used Matrix gave it rave reviews. "It's scary," one said. "I mean, I can call up everything about you, your pictures and pictures of your neighbors.")

Many at the expo knew that Justice Department and Homeland Security officials had budgeted millions of dollars for Matrix, possibly for use as an anchor in a national intelligence- and information-sharing system. Now police at the conference could see the fabled Matrix firsthand. All they had to do was sign up for a "law enforcement only" demonstration in the center's Liberty Ballroom, which they did with enthusiasm. For some police, the power of it was irresistible.

AFTER THE TERROR ATTACKS on September 11, 2001, our government leaders could not resist the promise that information technology would make us safe again. Even as the fires burned where almost three thousand people had died, they turned to computers, surveillance gear, and mountains of information about Americans as part of their nascent war on terror. This was an earnest impulse, shared by small-town police and G-men alike. If we could only know more about everyone, they reasoned, we would be able to discern the lethal few from the many good.

That fantasy had been brewing in the law enforcement world for a long time. It took a data revolution to make it feasible on an epic scale. Suddenly, after the terror attacks, the government was wedded as never before to the revolutionaries: the many information brokers, database marketers, and technology makers who had quietly amassed vast reservoirs of information about us and created tools to track, assess, and predict our behavior.

The collection of personal information has long been a part of American culture. The sweep and depth and pace of that collection took on dramatic new dimensions in the 1990s, thanks in large part to profound

improvements in computing and the advent of the Internet. Much of this took place out of the public's view, and largely without the public's direct consent. In some cases, data entrepreneurs sold their services to police as a way to streamline law enforcement. In many others, marketers simply wanted to know their customers better. They wanted to automate the process of customer relationships. They asked questions that could only be answered with more data. Who is someone really? What motivates people? How are they likely to behave? How can we get them to open their wallets? How do we separate the relatively few very profitable customers from the rest?

These questions are a lot harder than they might seem at first glance. To answer them, companies of all stripes went on a data collection binge, gathering, parsing, and shaping more information about more people than ever before in history. It wasn't just the credit bureaus or banks or those people who called incessantly at dinnertime. It was the Safeway or Vons groceries where you bought your steaks and beer and diapers. It was the CVS Pharmacy where you filled your Valium prescription. It was US Airways or American Airlines. The politicians to whom you donated money. The company that issued your Visa card. The publishers of *Vogue* and *The New Yorker* and the other magazines you read. The direct mailer who sold you sex toys. It was the company that gave you a toll-free number to make life more convenient, the electronic toll operator, countless World Wide Web sites and companies you've never heard about, who harvest data from surveys, public records, credit card applications, warranty cards, and so many other forms, like giant combines harvesting wheat.

That was only the beginning. New devices emerged that enabled mobile phone companies to say precisely where you stood on the planet. Grocery stores and banks began using electronic fingerprint readers to authenticate who you were—or give you the discounts you wanted. Tiny radio frequency identification devices, some as small as fleas, could be embedded in product packages, clothing, or even money, enabling another sort of tracking that was impossible before. Computer processors monitored the location and activity of cars. And computer software enabled individual banks to watch and assess every one of millions of transactions on a given day, looking for signs that you might be a criminal, a tax cheat, or have questionable ties to unsavory people

Cities and businesses and schools installed more and more cameras, some loaded with automated face recognition programs.

Almost everyone you do business with collected information about you, sold it to someone else, or sifted it for their own mercantile ends. In some cases, you eagerly sought out the benefits and conveniences they offered in exchange for your information. By now those bargains are being transformed, usually without your input, into a public-private security infrastructure, the likes of which the world has never seen.

THE GOVERNMENT'S TURN TO SURVEILLANCE was almost reflexive. Within hours of the 9/11 attacks, officials everywhere sought out private companies: Could they help track down the terrorists and bolster homeland security? Not since Pearl Harbor had the nation faced as devastating an attack. In 1941 and 1942, heavy industry responded with a massive boost in production of trucks, tanks, bullets, and shells. Now the government was asking Information Age businesses for a different sort of materiel. Swept away by a patriotic fervor, information technology specialists flung open giant computer systems across the country to help law enforcement and intelligence agencies search for clues about the nineteen hijackers and their accomplices.

Financial institutions gave access to credit card activity. Banks pored through customer accounts. Internet service providers helped trace email and account details. Data giants such as Acxiom Corp., ChoicePoint, and Seisint searched through billions of demographic and marketing records on behalf of investigators, often using thin threads of information about suspects to pull together hefty dossiers about their time in the United States. Northwest, JetBlue, American, and other airlines handed over manifests about passengers from across the country. Never mind the carefully crafted privacy promises, issued over the years to soothe customers.

At the same time, hundreds of companies followed through on a wartime tradition: they swamped Washington's bureaucracy with profitable proposals. Data mines. National IDs. Fingerprint readers. Sensors that can remotely replicate an agent's "sixth sense" of imminent trouble. The list goes on and on. Even in a nation long anxious about the specter of Big Brother, all this seemed to make sense to many people, at

least at the time. No one knew where the next attack would occur. Much of the country braced itself for atomic bomb explosions or the spread of anthrax. The White House said it needed to fight an unorthodox war. Counterterrorism authorities charged with keeping us safe said, over and over, that meant more data and more intelligence. The USA Patriot Act dramatically expanded the government's ability to eavesdrop and snoop with little public oversight. It is only one of many powers the government has invoked to collect information in the war on terror. The Defense Advanced Research Projects Agency even created an ominous new branch, the Information Awareness Office, which began work on a global surveillance system. "I'd be happy to trade off some of my freedom for security" became a common refrain. So intent was the push for security that few people contemplated, let alone questioned, the consequences of the government's aggressive acquisition of personal information and the sudden, fearful acquiescence of American citizens.

There's no disputing that expanded use of surveillance and dataveillance has helped the government in important ways. And it's no stretch to say information technology will be a crucial part of the war on terror for the rest of our lives. Authorities have detained scores of suspected terrorists, based on evidence they collected surreptitiously. They also are sharing information and intelligence far more readily, from small-town agencies to the CIA. That's due in part to pathbreaking networks and information systems, such as the Matrix, as well as to changes in law enforcement culture. But few people understand the true scope of these efforts, and for good reasons. Our leaders have often invoked national security concerns to cloak their activities in secrecy. White House and Justice Department officials declined to spell out publicly all the measures they're taking, even to Congress in some cases. Attorney General John Ashcroft, meanwhile, urged agencies to narrowly interpret requests made under federal Freedom of Information laws. The evidence is there, though. Many documents and interviews with business and government officials show that authorities have ripped through old restraints on government surveillance, often with the best intentions, certainly with new legal authorities. To be sure, there have been setbacks for the government along the way. Privacy advocates have hindered some projects, such as the Defense Department's Total Infor-

mation Awareness initiative and the Matrix, both of which came under intense criticism after becoming public. This resistance cut across ideological lines, but it is episodic and ad hoc. The drive for more monitoring, data collection, and analysis is relentless and entrepreneurial. Where one effort ends, another begins, often with the same technology and aims. Total Information Awareness may be gone, but it's not forgotten. Other kinds of Matrix systems are already in the works. And since the approval of the USA Patriot Act in October 2001, the Justice Department has never stopped seeking ever broader authorities, whether through a Patriot Act II or, as in the spring of 2004, demands for unprecedented access to communication online.

The government's ability to examine our lives is only going to increase in coming years, as the National Commission on Terrorist Attacks Upon the United States made clear in a landmark report in the summer of 2004. After analyzing the intelligence and security failures that preceded the terror attacks, the group, better known as the 9/11 Commission, called for standardized identification, widespread use of fingerprints and other biometrics, far greater information sharing, and a consolidated intelligence system. Such measures are crucial to our security, the Commission concluded, even though they will raise profound new questions about our civil liberties. "Even without the changes we recommend," the report said, "the American public has vested enormous authority in the U.S. government" [p. 394].

Surveillance comes with a price. It dulls the edge of public debate, imposes a sense of conformity, introduces the uneasy feeling of being watched. It chills culture and stifles dissent. By definition, it is often secret and hard to hold to account. That is why in the 1970s Congress shut down domestic intelligence operations that had led to so many abuses by the FBI, CIA, the U.S. Army, and others. It's also why it passed information and privacy laws. These not only restricted how the government could collect and use information about citizens. They required agencies to be more open. The new legal authorities and the government's partnership with private information companies now pose a direct threat to this three-decade-old effort toward openness. It's a simple fact that private companies can collect information about people in ways the government can't. At the same time, they can't be held accountable for their behavior or their mistakes the way government agencies can. Their capabilities have raced far ahead of the nation's understanding and laws. The legacy of these efforts will be with us for many years.

Peter Swire, who served as the nation's first privacy counselor in the Clinton administration, has warned that we're heading toward the creation of a "security-industrial complex." He intentionally echoed a famous phrase in the prophetic speech that President Dwight Eisenhower gave on the occasion of his departure from the White House in 1961. "In the councils of government, we must guard against the acquisition of unwarranted influence, whether sought or unsought, by the military-industrial complex. The potential for the disastrous rise of misplaced power exists and will persist," Eisenhower said. "We must never let the weight of this combination endanger our liberties or democratic processes. We should take nothing for granted. Only an alert and knowledgeable citizenry can compel the proper meshing of the huge industrial and military machinery of defense with our peaceful methods and goals, so that security and liberty may prosper together."

Swire, a business law professor at the Moritz College of Law of the Ohio State University, contends that national security is being invoked to justify measures that threaten some of the traditions—of individual privacy, autonomy, and civil liberties—that help define our national character. Behind these measures are self-interested companies—increasingly powerful private contractors to which the government is outsourcing many of the exigencies of surveillance and security. "You have government on a holy mission to ramp up information gathering and you have an information technology industry desperate for new markets," Swire said. "Once this is done, you will have unprecedented snooping abilities. What will happen to our private lives if we're under constant surveillance?"

ON MARCH 15, 2002, at a coliseum in Fayetteville, North Carolina, President George W. Bush beamed as the soldiers from Fort Bragg and their families chanted: "U.S.A.! U.S.A.! U.S.A!"

The memories of the attacks six months before were fresh. The president was there to spell out his plans for a long, relentless war on terror. "We want every terrorist to be made to live like an international

fugitive, on the road, with no place to settle, no place to organize, no place to hide."

It was a powerful moment. It also was an ironic echo to a warning from Senator Frank Church three decades before. Church had served as head of a commission formed to examine the nation's history of domestic surveillance. He had seen firsthand what can happen when law enforcement and intelligence agencies amass too much secret influence. In the late 1960s and early 1970s, some worked outside the rules, targeting innocent people and groups for their political views, or because someone mistakenly assumed an individual posed a threat. Church was especially concerned about the government's use of computers and eavesdropping technology. Such equipment, he said, could serve as a powerful weapon abroad. The use of it could also spin out of control, especially in the hands of tyrannical leaders.

"That capability at any time could be turned around on the American people and no American would have any privacy left, such is the capability to monitor everything—telephone conversations, telegrams, it doesn't matter," he said on a television news program in 1975. "There would be no place to hide."

Like it or not, the technology is now being turned on American citizens and foreigners alike. It is being deployed at every level of law enforcement and intelligence. It's vastly more powerful, varied, and sophisticated than Church ever contemplated those many years ago. As a consequence, the president's wish may come true, and the terrorist will have no place to hide. But then, there's a chance that neither will we.

1
SIX WEEKS IN AUTUMN

Assistant Attorney General Viet Dinh took his seat in La Colline restaurant on Capitol Hill and signaled for a cup of coffee. It was one of those standard Washington breakfasts, where politicos mix schmoozing and big ideas to start their days.

An intense foot soldier for Attorney General Ashcroft, Dinh had been in his job for only a few months. He wanted to make a good impression on others at the session and craved the caffeine to keep his edge. As he sipped his fourth cup and listened to the patter of White House and Hill staffers, a young man darted up to the table. "A plane has crashed," he said. "It hit the World Trade Center."

Dinh and the rest of the voluble group went silent. Then their beepers began chirping in unison. At another time, it might have seemed funny, a Type-A Washington moment. Now they looked at one another and rushed out of the restaurant. It was about 9:30 am on September 11, 2001.

Dinh hurried back to the Justice Department, where the building was being evacuated. Like countless other Americans, he was already consumed with a desire to strike back. Unlike most, however, he had an