The John Marshall Journal of Information Technology & Privacy Law

Volume 24
Issue 1 *Journal of Computer & Information Law - Fall 2005*

Article 2

Fall 2005

No Place to Hide, 24 J. Marshall J. Computer & Info. L. 35 (2005)

Robert J. O'Harrow Jr.

LECTURE

NO PLACE TO HIDE

by ROBERT J. O'HARROW, JR.[1]

MODERATOR: I wanted to begin with a quotation from a professor at New York University Law School named Bernard Schwartz. Some of you may have heard of him. He passed away some years ago. He wrote in his horn book . . . on administrative law . . . the following: "Our house may still in theory be our castle, but that castle no longer sits on a hill isolated by a moat. The modern castle is connected to a central water system, to a sewerage system, to a garbage collection system, and more often than not to houses on either side." If Bernie were still alive, he probably would write in his third edition, "and to the Internet as well."

Robert O'Harrow, Jr. is a reporter with the financial and investigative staffs of the Washington Post. He is also an associate of the center for investigative reporting. Mr. O'Harrow has written extensively about data privacy and has uncovered stories about uses of information that have led to changes in state and federal law. He was a Pulitzer Prize finalist for articles on privacy and technology and a recipient of the 2003 Carnegie Melon Cyber Security Reporting Award. In his recent book, *No Place To Hide*, Mr. O'Harrow explores how the government is teaming up with private companies to collect massive amounts of data on citizens and how, he writes, "more than ever before the details about our lives are no longer our own. They belong to the companies that collect them and the government agencies that buy or demand them in the name of keeping us safe." *No Place To Hide* details how computers are allowing businesses and the government to monitor us with very few regulations and virtually no accountability and how this information infrastructure will impact our traditional beliefs of civil liberties, autonomy, and privacy.

1. *See Biography: Robert J. O'Harrow, Jr.*, http://www.simonsays.com/content/destination.cfm?tab=1&pid=330578&agid=13 (last accessed Sept. 7. 2006) (stating: "Robert O'Harrow, Jr., is a reporter at *The Washington Post* and an associate of the Center for Investigative Reporting. He was a Pulitzer Prize finalist for articles on privacy and technology and a recipient of the 2003 Carnegie Mellon Cyber Security Reporting Award. He lives in Arlington, Virginia.").

This coming Sunday, William Sapphire will feature *No Place To Hide* in the cover article of the *New York Times Book Review* section. . . . Tonight, Mr. O'Harrow will share with us some of his views on protecting our personal privacy where there is literally no place to hide. Robert O'Harrow, Jr.

(Applause)

MR. O'HARROW: A few days after the terrible and unprecedented attacks on the United States, a fellow named Hank Asher was sitting in his expansive kitchen in Florida and wondering what he could do to help fight back. He was having a large martini, and he was chatting with a cop that he knew for many, many years. And it occurred to him that he had a special way that he might be able to help because he was a data savant who had invented some of the most cutting edge data collection and dispersion systems that there ever were.

In the 1990s, he created a system called Auto Track that collected information and shared it with lawyers and police and reporters and many, many others. And he was spectacularly wealthy as a result of that. After the terror attacks, he had another company called Seisint, which was short for Seismic Intelligence. And it had a storehouse then of about 20 billion records on every adult in the United States.

And the way he tells the story and others tell it, he rushed to his bedroom and started banging away on a computer that was directly linked to Seisint's supercomputers and worked well into the night and the next day and was able to identify what he said were several hundred people that the FBI and the intelligence services should target inside the U.S. And, in fact, some of the people on that list were on the planes that hit New York and Washington. And these were names that had not been released. So he had some effectiveness there.

Now, his story is especially interesting I think because not only did he have that data prowess and that special ability to look into the data, to do the data mining, but he's an unlikely soldier in the war on terror. A couple decades ago, he was a drug smuggler who carried cocaine and marijuana into the U.S. How do we know this? He told it to me. Police records show that he was a drug smuggler. At one point, he even conspired to fly down to Nicaragua and rescue mercenaries. He was an adventurer to say the least. Never charged. He said he hasn't done anything wrong since those days, and I believe him.

The fact is though that you have this rogue fellow who had this private company that very quickly attracted the attention of the Secret Service, the FBI, the Justice Department, the Central Intelligence Agency and for all I know the NSA. And his office in sunny Boca Raton, Florida, this private company quickly became an outpost on the war on terror. I don't think it takes a lot to sort of imagine some of the implications both

good and bad of those kinds of relationships. No one knew this was happening outside law enforcement, and it took a lot of elbow grease for me to find it out. I have a very high threshold for pain and banged away on the company's door for months and months until I finally started getting some details about this.

In any case, Asher continued to work on the system with help from all these federal agencies and with input, with data, with classified information, with law enforcement information that was poured into his computers so that they could make these queries that as far as I can tell were never possible before. Any one of you if you were an analyst could sit down at a Seisint computer that was hooked into this special system they were creating, make a query and for the first time . . . find out all the demographic information that the publicly held companies own.

Those are your real estate information, the car you drive, the licenses you have, the estimated income, all the people that you lived with in your adult lives, all the people that they know because they can make these linkages. This is all the stuff we are now sort of familiar with, all the data that's publicly available. Not only could they look at that, they could now look at all the criminal records, the investigative records, the files that only police are supposed to have, and they could look at it with one simple query. They could say a dark haired man who drives a car with six and an A and a Z on the license plate who looks to be in his thirties in the zip code 10016, and they could instantly come up with a list of everybody who fit that profile. If you want to add Muslim sounding names, they could do that. They could designate Hispanics. The point is it was a profiling machine.

The system that was created represents in many ways a milestone in what I call the data revolution. And this is something that people are becoming more and more familiar with. And the data revolution really accelerated in the 1990s when, as we all probably remember, we got our first PCs in the late eighties, early nineties. The price from that point on just plummeted, the price of data storage plummeted. The power of the computers exploded and more and more our computers were connected in these vast networks, not just the Internet but intra nets and public and private data switching systems of all kinds. This data revolution accelerated data collection to a degree that is very difficult for many of us to even grasp in a tangible way.

Here's one example. One company that went public in 1983 was at the forefront of this. This company was called Acxiom, A-c-x-i-o-m. It's based in Little Rock, Arkansas. From the point that Acxiom went public to the point that I was finishing my manuscript for *No Place To Hide*, they had approximately a million times more information about every adult American. A million times, that's a lot. They had at that point, and it's grown dramatically since I turned in the book . . . what I roughly

I calculated to be a 50,000 mile high stack of King James bibles. And this is information they can access instantly. They can take these dossiers, append them. Let's say you share . . . your phone number at the Radio Shack or Eastern Mountain Sports or whatever store it is, what they're doing is taking that phone number and they are appending all this other information to it so they can get a full, rich, 360 degree look at this customer named Bob O'Harrow or fill in the blank. That's the data revolution.

Now, why did this happen? It happened not only because it could happen because of the computing power and the networks. It also happened because of a shift, and I find this endlessly fascinating, in marketing strategy and the marketing philosophy. There emerged a philosophy that marketers really wanted to get to know you well. You were endlessly fascinating to them. They wanted to have a relationship, a customer relationship with you, and they wanted to manage you. There's a phrase, customer relationship management that a lot of us have heard. You can't manage a customer unless you know what cut of beef they like- if you like the ends, if you like filet mignon or if you like T-bone. There was a time way back when . . . our folks' parents went to the butchers, the butchers knew that automatically and they threw in a little extra piece for Rex, the dog, because they knew they had a dog. It made them feel good. They went back to this butcher. The customer relationship management marketing folks said, "We can replicate that on an epic scale." The only way they could do that, they said, was to have information about everybody.

And so they went on a data collection binge, and that's what helped drive all this information with this fantasy that they were reaching for that they could know everybody and serve everybody better. Give the discounts to the profitable people . . . but ignore the vast majority, the 80 percent who are not as profitable and serve everybody better. They could give them tailored jeans. Just sort of soothe our consumer souls. The only way they could do that is with the data, and so they collected the data. Then what happened? Well, they realized we could do fraud detection. We can find out, with all this data we can find out who is going to welsh on a debt, who's going to file false insurance claims. Then they realized wait a second, we can check who the pizza delivery people are. Do they have a criminal record? We can check on volunteers. We can accelerate police investigations. Police are among the biggest users of this stuff, these private companies. So you have this marketing movement that just kept morphing into fraud detection, into law enforcement and, in effect, into private intelligence.

One of the companies that a lot of you have heard about is called Choice Point. Choice Point is a company based outside Atlanta and is a remarkable company. And it's worth watching them not only because of

their huge security breach recently but they're just fascinating as a business because they are relentless in their desire to grow. What do we mean by that? In 1997, they spun out of one of the credit bureaus called Equifax. They were a division of Equifax, and they had about 1,000 customers. They went on an acquisition binge to buy all the other information companies they could get a hold of, including one that Hank Asher used to own. Made him rich when they bought that company.

They soon acquired companies that had not only public records and billions and billions of records, not to be a broken record on that, but it's a big number. They bought companies that control birth certificates. In 50 states now, there's a company called Vital Check that Choice Point owns that now resells birth certificates. So you don't go to the hospital anymore. You go to Vital Check and you get your birth certificate that way. Death records, marriage records, all that sort of stuff. So they own that. They bought companies that maintain blacklists of people that have been convicted or accused of shoplifting.

They maintain the database, and it's a cooperative. Target. . . Wal-Mart, others, I believe Wal-Mart's a part of it. They contribute these names. So even if someone has been referred to police as a shoplifter, they're in this database. And as Choice Point points out in its marketing material, the companies cannot be held liable if they're wrong by sharing this information unless they knowingly were wrong.

In any case, they bought 58 companies and they now have something in the order of 100,000 customers. It's 1,000 in '97, 100,000 now. They started out with $500 million in the value of their stock. They're worth over $4 billion now. Some of their more recent acquisitions I think are particularly telling and tell us where the company really wants to go. They bought a company called I2. The name won't mean anything to you but what I2 does is it takes the ocean of information, looks in it, and it could map how all of us are related. It could show through links how I know you or how we're related through five other people. They can show that automatically and graphically display it.

I2 is one of the great tools in the war on terror. In fact, it was used to hunt down Sadam Hussein on a tactical basis. It was on the laptop computers that the Army, Special Forces or whoever it was that captured Sadam Hussein. They mapped some of these relationships and realized that he's probably in this town. There's a real utility to I2, but it showed that Choice Point had greater ambitions than the U.S. because I2 customers are all over the world. In effect, they had become one of the world's largest private intelligence operations.

Likewise, Lexis-Nexis. . . . The lawyers and business folks in the audience, the journalists if there are any here, everybody depends on Lexis-Nexis. They have wonderful service, billions and billions of news-

paper articles, legal documents. What people don't realize is . . . that Lexis-Nexis is also becoming in effect a private intelligence service. Guess who bought Seisint, Seismic Intelligence, the company that I started discussing? Well, Seisint went on to create a system that you may have heard called the Matrix, and that's this, in effect, a truth machine, a data profiling supercomputer extraordinaire. Well, guess who bought them? Lexis-Nexis. Most people don't realize that Lexis is a major intelligence and homeland security player.

Why does all this matter? Some of you may recall that when Dwight Eisenhower left the government, when he was leaving the White House, he gave a speech that to this day resonates, I believe. I find it very moving particularly because he was a war hero, he was a mainline, as mainline a Republican as it comes, and I'd like to read you a section here about what President Eisenhower said. He said, "In the counsels 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 when he was leaving the White House. "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."

Well, I propose that we change military, industrial complex to security, industrial complex and start recognizing that what the government is doing when it goes to Choice Point or Seisint or Lexis-Nexis and a whole array of other companies that none of us have ever heard about-information companies, software companies, data miners. I propose we call it a security, industrial complex because these relationships face very little accountability. We can't know what they are. There's nobody watching these relationships. We have no control over how the government uses the information. And on top of everything else, government is, in effect, by out sourcing to these companies with $50, $100 million contract, they're sidestepping rules that were put into place two generations ago or back in the seventies to sort of put checks on the government from doing domestic surveillance, from intruding into the political and personal lives of American citizens who've done nothing wrong. I see this as a major challenge and one of the things that's the most compelling about these developments.

I'll conclude with one thought here, one passage from the book and then what I'd like to do is maybe answer some questions and just discuss this a little bit. 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 "USA. . .USA. . .USA." 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. President said, "We want every terrorist made to live like an international fugitive, on the road with no place to settle, no place to organize and 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 the head of a commission formed to examine the nation's history of domestic surveillance. He had seen firsthand what could happen when law enforcement and intelligence agencies amass too much secret influence. In the late sixties and early seventies, some of those officials 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. Church said that capability at any time could be turned around on the American people and no American would have any privacy left, such as 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 terrorists will have no place to hide. But then there's a chance that neither will we. Any questions? Shall we talk? Yes?

MALE SPEAKER: How do you answer the questions if you express your concern about . . . privacy and their response is, "Well, if don't have anything to hide, why are you concerned?"

MR. O'HARROW: It's a —

MALE SPEAKER: It's a disgusting response . . .

MR. O'HARROW: Well, I don't know that it's a disgusting response. It forces us to articulate things, which is what we're all supposed to be doing anyway. My response is this. The simple idea, the easiest first step is to say there are mistakes. We know there are mistakes. How do we know that? Has anybody heard of Brandon Mayfield? Does anybody know Brandon Mayfield? Brandon Mayfield was a lawyer out in Oregon . . . who had converted to Muslim. . . . He was targeted by an international manhunt, in effect, because a fingerprint was found on a plastic bag after the terror bombings in Madrid. It was Brandon Mayfield's they

said. Even though the machines were not sure and the people, the FBI agents were not sure, Brandon Mayfield was thrown into jail, and we learned today in the Washington Post that using secret Foreign Intelligence Act warrants, they went into his house and took hundreds of photographs, 350 photographs, they got cigarette butts and got genetic information. They got tons of details. Turned his house upside down.

Oh, but they were wrong, and the FBI apologized. It's a mistake. Do you think there aren't going to be people who are going to think Brandon Mayfield for the rest of his life was a terrorist and they're going to steer clear of him? There are mistakes in the data. The data in these information systems is so completely filled with mistakes. Doesn't obviate the benefits. Let's be real here. We love the benefits. We love the cell phones. We love the ATM cards. We love the credit. We love the mortgages. There's a lot of benefits to be had here, but we must realize that these data systems are filled with mistakes to the degree that the FBI even announced several years ago it couldn't comply with a federal law that required them to certify that the databases were free of mistakes. They said we can't do it. On the record it was an announcement. That's the first easy step. Okay, why does it matter if you have nothing to hide?

Go to another extreme. I honestly worry that we have this constant, ceaseless struggle with conformity in the United States. I believe that I like the people on the flaky edges. They're the ones that show us sometimes mistakenly where we should be going, how to think, different ways of viewing the world. They're amusing, they're challenging. To me that . . . makes American society great. I honestly fear that the more we understand how much we're being watched, the more we're going to fall back on our heels and fall prey to the tendency that I think we're all too afflicted with to be conformists. And to me that's a shame, and it's going to change the nature of our society. In between the mistakes and the conformity, there are all sorts of—there's a bunch of lawyers in here who could just parse this endlessly better than I can, but there are all sorts of due process issues. How do you fix a mistake? Are we going to cede control over information and gate keeping to these private companies? That's why it matters, and that's what I would say.

And here's what—I'm from Indianapolis. When I was a kid I was there, and I remember hearing this phrase, and I've been using it to great effects in an "aw, shucks" kind of way, but the fact is it's true. I remember hearing my folks say in effect, "Who the hell gave them the right." And it could have been a neighbor doing something or whatever, but it comes to mind on this. It's who gave them the right. Let's take stock of this and try to get things back in balance because I think that a lot of these companies are overstepping the bounds of civil society. Even though it's perfectly legal and even though we like the benefits, they've

overstepped and I think that we need to try to find the right balance so we get the benefits and we minimize the downsides.

Yes, uh-huh?

MALE SPEAKER: In any event, I think you should, when you discuss this subject you should pay homage to Louis Brandeis who wrote his famous article in the Harvard Law Journal before the turn of the century defining what the Fourth Amendment was. And ultimately you already have.

MR. O'HARROW: No, it's something —

MALE SPEAKER: Ultimately what Brandeis boiled it down to was the right to be left alone. And the Supreme Court decisions that followed thereafter upheld that. That became, in effect, as far as law and the society was concerned, a guiding principle. And you mentioned the Church investigation into what the government was doing, probing into the lives of private individuals and governmental officials. That was a re-establishment of that principle. However, in a very short period of time, and maybe it was all due to technology, we have gone a long, long way from that, and privacy doesn't mean anything anymore.

MR. O'HARROW: Well, privacy does mean something. And I believe and I want you to believe that we're at the very, very beginning of something and not at the end of something. Don't believe people who say you've lost your privacy, get over it. That is facile, anti-intellectual posture. I think that's silly. We're at the very beginning of the data revolution, and we have to come to grips with the complexities here. I challenge anybody in the room to tell me that there aren't benefits, enormous, extraordinary benefits from the Internet, from data mining, from all this stuff. To me it's amazing. Cell phones, it's an amazing thing. We're not going to give those up and we shouldn't. Likewise, I believe we should use information technology to the greatest degree possible to protect the country and to make the country safe or to create a space where we can do art, do business, learn, raise our kids in a safe way.

The question that I am trying to confront is how . . . we do that without erasing some of these values that Brandeis articulated so well without creating new sources of power that can be used in ways that are unaccountable. To that end, I wanted to mention something that I think is an even more core issue for my book even though I, of course, mention the Brandeis business as well. But relating to this notion of unaccountable power which is what Eisenhower was talking about, you might recall Brandeis said men born to freedom are naturally alert to repel invasion of their liberty by evil minded rulers. The greatest danger to liberty lurks in insidious encroachment by men of zeal, well meaning but without understanding. To me that's a very big force at play here right now.

Yes?

MALE SPEAKER: I wanted to know how the data that they have from Echelon, the NSA illegal domestic spying, now with the Patriot Act, it's redefining things like your lawyer and your travel agent as financial institutions so they can get the records without a warrant. Are they going to, you know, mesh the data they gather through Echelon with these current systems?

MR. O'HARROW: It's hard to know. I think that would be illegal if they did that. I kind of doubt it, but it's hard to know. I mean, you know, I don't know FISA, Foreign Intelligence Surveillance Law well enough, but I'm quite sure that Echelon is focused on other countries. But there is a lot of data collection going on as you know. And it's everything from so called business records to the cars that are rented, hotels. And these are big electronic sweeps, and they're taking the data and pouring it into data mines to look for patterns that might represent a terrorist threat.

By the way, one of the people I spent a great deal of time with on the book, great deal of time relatively speaking, was John Poindexter who was overseeing the Information Awareness Office and the Total Information Awareness Project. And I specifically think of John with that Brandeis quote of zealous people because he's a zealous guy. He's a brilliant, brilliant fellow who considers himself deeply patriotic and, in fact, I think he is. And yet his focus and the likely success in many ways if he were allowed to proceed is unsettling because so much of what's being done in the name of national security and protecting us is being done earnestly, but it's so far beyond our understanding and our laws.

And what I'm trying to do and I imagine what a lot of you are trying to do, and there are some law students in here who are studying these issues, is not say let's put the genie back in the bottle because I don't believe that. I believe we should embrace the benefits, but we have got to do the very heavy lifting first to understand the scope of all of this and then to figure out how to do policy and regulation well so that we can protect something that is so core to America which is we believe in the autonomy of the individual. We believe that the individual is an important part of our society and that there are some inviolable boundaries that should be there.

Yes? Back there.

MALE SPEAKER: My question concerns how all this information from this data revolution affects us with regard to private companies. I mean certainly you've outlined some of the risks involved with the government and mistakes that can be made with that. Well, what about private companies using this and when you get into things like trying to get healthcare or getting financing and a certain part of the public could be marginalized or excluded access from some of these basic services?

MR. O'HARROW: Well, they are. They are being excluded. Discrimination is built into this, and I don't mean discrimination as a buzzword for discrimination against women or discrimination against men from the South or African Americans from Massachusetts. But I mean literally looking at millions of people and saying these 20 percent show the signs of future profitability. These 80 percent we want to spend as little time and energy on them as possible. We're going to focus on them. They're making those kinds of choices more and more. For insurance, insurance companies are looking into this data. Choice Point is one of the main ones on this. They look into data and they make determinations based on your perceived history, on records that may or may not be accurate. Probably for the most part they are. They're coming up with scores. Everybody has heard of FICO scores, right? That's for your credit score. There are scores now for more and more things. Lexis has scoring. There's a company called HNC that works with . . . the originator of the FICO score. HNC is artificial intelligence. It can look through, oh, there's that word again, billions and billions of credit card transactions, and they're constantly monitoring this for signs that you might be a thief, somebody's using the account inappropriately or that you're a terrorist. And decisions are being made based on those scores to say in or out, yes or no. You can be a volunteer or you can't.

I'll give you an example. After 9/11 a lot of companies decided they'd better do a better job checking out their employees. After the fact, looking at employees that were already there, they went and found that some of them had bounced checks in their prior lives. Somebody had a pot bust. There was all sorts of—one was there was an allegation of domestic violence. Guess what? Bam, they're out the door. They're gone. And I just find that amazing because maybe in some cases that's appropriate, but at what point do you grow beyond a $60.00 bounced check. And how do we know that you were to blame for the check being bounced? How do we know it wasn't a misunderstanding because it's out of context? But there it is. It's in writing. It's technically accurate, but out of context-what does it mean? There's a fellow named Chris Hufnagel who came up with a really good, important phrase that doesn't help us on the intricacy of the law, but it gives us a kind of big sweeping framework. He used a scarlet letter society. Choice Point, by the way, I can't urge you enough to read the chapter, but go and just look them up on the web. Choice Point's CEO is a fellow named Derek Smith, and Derek Smith's a very competitive guy. He oversaw the acquisition of these 58 companies. He's competitive because he was a college athlete. He's a scratch golfer. Derek, after 9/11, his compensation grew by 50 percent. In 2002 it went up to $20 million. And at the same time, he believes that he's on a mission, spiritual mission in his words to apply Choice Point technology to make this a safer country. He's a Presbyterian by the way.

(Laughter)

MR. O'HARROW: He's very open about this. There was a special, a Peter Jennings special, and I interviewed him for that. I'm the guy behind the camera. It was kind of cool. But I'm talking to Derek Smith on this interview, and he talks seriously about wanting to be the gatekeeper, Choice Point, now get this, he wants to be the gatekeeper to enforce the rights and privileges that every one of you is claiming. I want a job. I want to travel. I want to go to this hotel. I want to be a volunteer for my kid's soccer team. I want to work as a pizza delivery person. I want to go to the FBI. I want to get into Madison Square Garden. He wants to be the guy that is the gatekeeper that makes us all safer by having this data that's checking us out constantly. I just find that just stunning. I mean, I don't know. I just find that a stunning thing. And guess what? It works. Millions of companies use them. . . . many of the major Fortune 500 corporations, most of the federal government agencies, at least 2,100- it's probably 3,000 law enforcement agencies around the country. I got Freedom of Information, people have heard of that. It's a painful process because your former Attorney General told government agencies to, in effect, ignore the spirit of that. So it was really hard on my project. One of the responses that I did get came from the CIA where they acknowledged that Choice Point and Lexis-Nexis were contractors. The CIA is contracting with Choice Point and Lexis-Nexis to look at data about 220 million adult Americans. Somebody's got to do the—any journalist in here please do the follow up story. Come on. You know, why are they looking at domestic? I thought there were limits on domestic surveillance. So I didn't have the time and—yes?

MALE SPEAKER: With all this money and effort that these companies are (inaudible), how is it possible they could know what toothpaste you buy, but they can't find a six-foot tall guy who needs dialysis who's out in Islapaga or wherever he is? How come they can't find Bin Laden then? I mean if they can find you if you go to (inaudible)?

MR. O'HARROW: Okay. You've raised a very good point. You've raised a point that, interestingly enough, marketers raised. Marketers will tell me what are you worried about. We are overwhelmed with data. Now, I just love the logic here. We're overwhelmed with data, which I don't doubt. We're at the early stages. Remember that? We're at the very beginning of this. If they're so overwhelmed, why do they have a million times more data than they had when they went public in 1983? The point is because they are becoming more effective- it's really flawed. It's really imperfect. Now, to me, I take the fact that it's flawed as even a little bit more unsettling because that means they're going to be like the Jolly Green Giant kind of stomping around with all this data, and there's going to be people who are going to get stomped under those big feet by accident because it's not as refined as it should be. And by the way, some

of you are probably thinking, well, maybe that's a good thing because the technological barriers will serve as checks on these companies. To me, I think that's foolish. I don't think we should have policy by ineptitude. I think we should have policy and regulations that are well thought out and don't depend on the technology being imperfect. It is imperfect. They can't make the most use of this data as they would like or sometimes claim, but they're a hell of a lot better than they were two years. And they're light years better than they were ten years ago. And go back 25 years and what they're doing now is science fiction.

Yes?

MALE SPEAKER: So is it your opinion that government agencies can get immunity from their laws on contracting information from private companies? So they can get information from these companies that they're not allowed to gather on their own?

MR. O'HARROW: Yes. Well, I don't know if it's immunity, but it's just legal. Right? There's no law that I know of. After 9/11, some of these agencies asked their lawyers, and I'm going to see if I can find it really quickly here cause it's kind of interesting language, they asked their lawyers, you know, can we use this. And a group called the Electronic Privacy Information Center, it's an activist group in Washington got some stuff through for you. And let's see here . . . U.S. authorities felt comfortable using—page 153 for those of you who have the book—felt comfortable using Choice Point's services. Shortly after the terror attacks, the FBI Office and the General Counsel ruled in a classified document that it was perfectly fine to rely on data for foreign intelligence collection or foreign counterintelligence investigation. The documents concluded that "individuals do not have a reasonable expectation of privacy in personal information that has been made publicly available." So they could go to these companies and outsource and they did. And the Justice Department for one after 9/11 signed a $67 million expanded deal with Choice Point to service all their agents.

MALE SPEAKER: So far I've heard little or nothing in the presentation about real sanctions for the abuse of this data collections. If Mr. Smith was stripped of $20 or $30 or $40 million dollars for the egregious use of this information, you might get the message. If there were exclusionary lawsuits, we have other areas of the law where the government misuses this information and it gets thrown out, we will have maybe some results. But I haven't heard any—I mean everybody's talking about, oh, this is terrible. Well, hell, yes, this is terrible. We all know that.

MR. O'HARROW: Well, it's not all ter—I'll interject. It's not all terrible but —

MALE SPEAKER: (Inaudible) positive aspects, but the —

MALE SPEAKER: Oh, yes, it has.

MALE SPEAKER: —untoward results of where it goes wrong such as your example with the attorney up in the Northwest is draconian.

MR. O'HARROW: Here's the—I have a little bit of a skeevy sort of backdoor thing that I do which I'm a reporter. And I felt that my job was to do what Brandeis called "shining the bright light," you know. What is it? Sunlight is the best of disinfectants, a bright light the best policeman, to paraphrase him. My backdoor is not—policy is not schtick. Regulation isn't. That's going to be for the smart lawyers in Washington and all over hopefully the state capitols. What I'm hoping we can do is engage in an understanding of the complexities, recognize that the benefits are intertwined with these things that I find very, very troubling- the sources of power outside of accountability, the chilling effect on politics and on society and on free speech and all the rest. I want to try to limn that as clearly as possible to show that it's not paranoid since I'm probably the least paranoid person in the room. It's not a conspiracy. It's things as they sort of—it just developed and we need to confront it. Here's an analogy by the way. All right, so I'm not going to do policy. If somebody wants to talk about it I'd love it, but I will tell you there's an analogy that I've been chewing on and as imperfect as it is, it seems to help me a little bit. Let's go back to, does anybody remember the—well, they've heard about Gary, Indiana not far from here back in the fifties. Apparently, it was dim on the brightest days because the pollution was so bad. Rivers in Ohio catching fire, a river in Ohio catching fire. The air in a lot of cities, in L.A. just being so smoggy that people took emphysema and respiratory diseases, just took it for granted that somebody they knew would have that. At the time, everybody just took it for granted or most people did because it was part of our quality of life. If you told the coal burning energy producers or the manufacturers that created all this pollution that you have to do something about it, they'd say the hell we do. We would have to shut down. We can't do this. Your quality of life would fall if we have to follow any set of rules. Well, guess what? The air is much cleaner than it was because we came to a recognition in society that this is a bad thing. People didn't have to necessarily die because of a quality of life, that we were going to have to sort of figure out a way to structure this so that we could still have manufacturing and energy and so on with less pollution. We figured it out to a much greater degree. It's not perfect, but it's better than it was. I propose that we can figure this out as well, that we can come up with some solution, that it's not hopeless. It's far from hopeless, and that in the same way that I think of identity theft, for example, as the pollution, the eternality that we need to address. And it's only the obvious one.

Yes, in the back.

MALE SPEAKER: Now, I just wanted to get your comments on two competing cultural impulses and privacy. I'm talking about this need for regulation and defense of privacy at the same time, a lot of the same people are making their information public through blogs. There's a steady increase in blogs. So it's this kind of idea that you can have my heart and soul but not my credit. And, all right, and what does that mean to this.

MR. O'HARROW: Well, to me, I get deeply, deeply annoyed by people who make that argument. There's a very, very different thing when you say I'm going to express myself and it may be express myself is that I like sex this way or I like these kinds of movies or, you know, something really personal. Okay? You're choosing to do that. It's an exhibitionist impulse. Big deal. There's a very different thing between that and companies deciding, oh, he's probably an exhibitionist. I'm going to learn everything about him, and I don't have to tell him because I don't have to. Right? I'm not going to tell him because I don't have to. It's a very, very different thing. Now, there are people, there's this weird civil libertarian twist. You get all sorts of grades here. You have the left and the right hands across the water on this issue, but you also have like a civil libertarian part that says, you know, we are a nation of exhibitionists. Why worry about it? Well, because it's not really about privacy. It's about autonomy. It's about choosing and having some circles of autonomy around you, not just defaulting because we don't know about it to private companies that have decided they're going to learn absolutely everything about it and then push those buttons to try to get you to open your wallet as much as possible. Or more and more people get you to choose, make certain political decisions. The political parties are starting to use this stuff a lot more, and we're really at the very beginning of that. Acxiom, Info USA, they maintain a database of Democratic voters called Demzilla. The Republicans are bragging all over Washington about how good they are at using these data systems. And they're doing it in like a real sneaky, smarmy, you know, sophomoric way like, ha, ha, if they only knew. Well, eventually they will know. And do you understand? Am I making the distinction clear that it —

MALE SPEAKER: Yes, you are. And I don't think there's—I just think it's interesting in a way today we might value privacy but if I think autonomy is —

MR. O'HARROW: Right. Autonomy is a really important different thing because people want—a lot of times you're going to also hear people trying to convince you that anonymity is the same as privacy. Well, that's ridiculous. There's a company out there that was just bought by IBM that is funded, I'm not making this up, by an outfit called Incutel which is a CIA venture capital firm. Incutel funds this company, gets bought by IBM. This company called SRD is coming up with a system

that would anonymize data so that for counter terrorism purposes, they would anonymize data from hotels, from cruise ships, from rental car agencies, you name it. But it could be library records. It could be all this stuff, and they would put it into a giant ocean, a giant data ocean, and it would all be anonymized. And they are claiming, oh, it's anonymized, therefore, the privacy problem is solved. In fact, it's quite the contrary because it's not about privacy. It's about autonomy and it's about surveillance. All it does is it'll accelerate the government's ability to do surveillance because it's the government that will get to decide to de-anonymize it if it meets one of their profiles. Do you follow the logic? So it's actually going to accelerate it because we're all going to be sitting back saying, oh, thank God, the privacy issue's solved. It's anonymized except it's the government in an, I would argue, almost certainly unaccountable way or lightly accountable way, certainly outside our ability to understand what's going on. It is going to be the one that says, well, this meets the threshold to de-anonymize it, and all of a sudden they just like, okay, let's look at these thousand people. They de-anonymize it and it's all there. So where's the benefit? There's one little narrow benefit so that you don't get hackers going in and stealing it.

Yes?

MALE SPEAKER: Given what you know about data mining and data collection, do you do anything personally to manage or safeguard your own personal data?

MR. O'HARROW: Well, yes.

MALE SPEAKER: I'm talking about privacy or not having —

MR. O'HARROW: I do but it's very practical. I said, and I know I always get a little laugh out of it, but I really am like a totally non-conspiracy theorist. I believe in just—I don't believe anything pretty much unless I check it out. So if there's a conspiracy theorist, it's like, ah, you know, shut up, you know. But I check everything out, and I'm just not paranoid, but I do have good information habits that are enhanced by a diligent wife shall I say. So we tear things off the mail and you tear up documents and stuff because identity thieves are very opportunistic so if there's a trash bag filled with your social security number, and it says please go to this place to steal my money, they'll do it.

(Laughter)

MR. O'HARROW: All right, so that's the information habits. You got to have good information habits. Don't, please, dear God, don't share your social security number with the clerk. The clerk, first of all, has no clue why that clerk is asking you for the social security number. They're only doing it to build these dossiers, and if you want to have the relationship, start dating. You know, start dating the corporation. Let's go out for some, you know, pizza and a coke. But don't. They're back dooring it.

Just say no to that, and don't fill out warranties. These are practical things. You don't have to fill out warranty cards, people. You get the warranties. It's a law. The surveys. If you want to feel special go to a spa. If they tell you you're going to be a special customer, come on. You can do without the, you know, four-cent, you know, vial of perfume.

MALE SPEAKER: One more question.

MR. O'HARROW: Yes?

MALE SPEAKER: The (inaudible) Choice Point and Lexis-Nexis.

MR. O'HARROW: Yes?

MALE SPEAKER: These are companies, they brought the (inaudible) only after 9/11 or?

MR. O'HARROW: No, no, before 9/11.

MALE SPEAKER: Before 9/11?

MR. O'HARROW: These relationships were building all the way through the 1990s and they expanded and they intensified so that not only they give broader access to data, they provided analytical tools that were more intelligence oriented.

Yes?

FEMALE SPEAKER: What (inaudible) for a recourse? Recently, Choice Point was supposed to inform people of if they had a hacking on their system or a (inaudible). And they were supposed to inform individuals that their files could have been accessed. And so depending on what state you lived in, you received your letter and if you lived in another state, you didn't necessarily receive it.

MR. O'HARROW: Well, actually, no. They said they were going to send letters out to all 145,000 people regardless of where they were.

FEMALE SPEAKER: Okay. But what recourse do you have if, for instance, that wasn't let out in the media about that happening and the company such as Choice Point, what if they decide they don't necessarily have to reveal that?

MR. O'HARROW: Well, there you are. I mean there's one of the gaps which I and it looks like half the country find, you know, very troubling. There's this company, Acxiom that I've brought up several times. Acxiom may have the most data of Americans of everybody. They had a guy, a young guy who was working as a subcontractor to Acxiom and had access to their data systems. The guy loaded information about 20 million people and had them on stacks of CDs and started talking online about maybe selling this to identity thieves. Apparently did do it, but Acxiom came out and said, when it became public—the guy was just sentenced recently—but Acxiom came out and said, you know, we didn't feel like it rose to the threshold where we needed to notify our customers. Well, guess what? They were talking about their customers. They weren't even talking about us. So they never did go and inform the indi-

vidual people that their information had seeped out into the world. And that was another case where they have this display of security and so on, but these companies, there's no auditing that takes place.

There's no outside accountability even though Acxiom was a prime contractor on something called CAPS II. Does anybody recognize that? CAPS II was the system that was going to screen every aviation traveler secretly in a classified system and establish your rootedness in the community. They were going to profile every traveler, and there's something like 700 million travelers, some of them the same people obviously, a year. They were going to profile those every single time and decide if you showed the attributes of a proper American who's properly rooted. And if you didn't, you were going to get extra screening. So this is all complicated by 9/11 because you have this security, industrial complex emerging and you have the marketing and the private sector stuff all sort of blending together.

Yes?

MALE SPEAKER: There was a program on C-SPAN covering the Senate Banking Committee who was interviewing the individual who's a Vice President of Choice Point.

MR. O'HARROW: Uh-huh.

MALE SPEAKER: And had we not had the law from California —

MR. O'HARROW: That's right.

MALE SPEAKER: —none of us would have even heard about Choice Point.

MR. O'HARROW: No. No, I had a very anxious TV producer. It was kind of funny. We did this segment on *No Place To Hide* on Peter Jennings in January, and we had a long interview and it was a great interview and it worked well with Derek Smith. But Derek Smith didn't say, "Oh, by the way, can you get this on camera, we accidentally gave information out about 145,000 people." He didn't bother. He claims he actually didn't know. If he didn't know, that's troubling, and if he did know that's troubling. But be that as it may, this producer was very upset later because he's like why didn't we have that, and I was explaining that if we had had it, it would have been on the front page of the Washington Post right away. So the fact is they told us only because of that law, and then somebody who got one of those letters went and told us in the media.

MALE SPEAKER: Well, the one senator who I believe was in charge of the committee stated to this Vice President of Choice Point that receiving letters from his constituents, one individual purposely said his recourse should be that he has a property right in his personal information and that Choice Point should be taken to task, give him moneys for his,

like he had 1,800 hours involved in identity theft because of their screw up.

MR. O'HARROW: There is a property rights analysis some people try to do on the data, but I'm not an expert. There's probably some in the room here, but that bumps very head up against a tradition that I find fundamentally important in the United States which is public records. Without public records, how do you hold accountable public officials? How do you find out who is owning the real estate? I mean one of my first big stories was looking at public officials in a small town that were bringing in a sewer line from another town, and it was really important. It was going to transform the town and, you know, make everything safe. The local lake was not going to be polluted anymore by septic systems. Well, guess who was buying up the land along the sewer line that was zig zagging through this town? A consortium of different partnerships . . . of these officials. I wouldn't have found that out unless I could go to the real estate records and just keep pulling. If you have this property right, we would lose that sort of accountability which is a value that we hold dear and ought to hold dear and is a fundamental source of information for the media which, say what you will, we're all very happy when the media does its job and holds these people accountable I believe. I know you're happy with me.

(Laughter)

MR. O'HARROW: Any other questions? Yes?

FEMALE SPEAKER: Credit bureaus like TransUnion invite us to check our credit records and then track them. So I was wondering if there's any way, and even they like to say, "Oh, you can improve your credit." Let's say even if you went bankrupt. Is there anything, if we can't buy this information, is there anything we can do to, say if we think you might have already given out too much information, is there anything we could do to like counteract some of the things that we might fear?

MR. O'HARROW: Well, there are people who —

FEMALE SPEAKER: By putting more information in like (inaudible).

MR. O'HARROW: Well, there are people who recommend, and I don't, you know, I'm not of this ilk, but there are people who try to come up with variations on their names, and they turn their address upside down and all that sort of stuff. Well, do you remember the company I mentioned that's funded by the CIA called SRD? It was bought by IBM, and they have this anonymizing system. Well, the anonymizing system is a variation on another system called Non-Obvious Relationship Awareness, and I'm not making that up. That system can look at 10 million records and know when this record and this record are actually

the same person, even though in this record they twisted the information around. It can put those records together and say that person was trying to obscure the relationship or to hide the relationship.

Is that—it's pretty wild. And by the way, this guy, Jeff Jonas, he's a character. These are all characters. By the way, just in terms of selling the book to you guys, it sounds like it's all about computers and networks, but it's really not. It's about people like this guy, Jeff Jonas who came up with that system. Jeff Jonas is a high school dropout, who is a tri-athlete who is a gazillionaire now, who is based in Las Vegas and is just this wild man who regularly flies back and forth from Vegas to Washington because he's constantly meeting with the NSA with whom he has a contract . . . He was an advisor to John Poindexter and is constantly in this black world of intelligence. In the book, John Poindexter is there and Hank Asher, the one-time drug smuggler. It's really about characters and so on. So that's one thing you could do, is you could try to obscure that, but if you come up against a company that's using NORA, Non-Obvious Relationship Awareness, you know, it won't help.

And the bigger answer is no, there's not a hell of a lot you can do because you don't have control. Well, when I was introduced, he read this line from the book, but I think it bears repeating, and it's a really interesting thing if you don't mind me reading just a passage here. But it's kind of cool. Hang on one second here. I was walking around New York with a guy named Richard Smith, and this guy is a serious geek and knows the technology and has the technician's kind of mask, but he, in fact, feels passionate about American history and about what all this means. And he was giving me a tour of New York at my request and showing, walking through Manhattan and driving through Manhattan all the sensors that are collecting information on us now. It's a fantastic thing. It was a great exercise.

So we're walking through with Richard Smith, who's another character. And, oh, by the way, he has chops. The guy's a serious character, and that's why I used him as a character in the book because he identified something several years ago that some of you might have heard about called web bugs which are like cookies except you don't detect them in the same way. They're embedded in a web page, and they help track where you're going from Web site to Web site. He detected in Word documents, Microsoft Word, that there's a coding in those electronic documents that can be traced back so you can follow who's had that document even at the end stage. They can tell who's had that electronic document. So if you e-mail it to a friend and they work on it and so on. So he really knows his stuff. And we go through Manhattan and he points to a Porsche and it's got a GPS thing. He points to the cellphones which are tracking devices now, you know, and they can establish time and place. Fingerprints, ATM cards, of course, the camera in Starbucks

above the shoulder of the clerk. It's a little cube, WiFi. Now, we love this stuff, but it's all—these are what he calls sensors, and they're everywhere and the data's starting to converge, right, from each of these sensors to track when you get on. Those cards that you use, you know, in Manhattan and Washington, you swipe it, it records the time and place that you swiped it. And if you bought it with your credit card, it knows it's you. So if you throw it away and a cop or somebody picks it up or a hacker, they know that that was you and exactly where you went, all this stuff.

So he's showing me this stuff. And at one point, Smith shook his head at the idea of so much scrutiny, but as he stood on the street not far from where almost 3,000 people died in the terror attacks two years before, it was clear he had no illusions. The more computer space we have, he said, the more likely it is we'll fill it up. That's just the nature of things. Just as likely as the government's increasing reliance on the many details we leave behind in the routine course of our lives. Law enforcement and intelligence services don't need to design their own surveillance systems from scratch. They only have to reach out to the companies that already track us so well while promising better service, security, efficiency and perhaps, most of all, convenience. More than ever before the details about our lives are no longer our own. They belong to the companies that collect them and the government agencies that buy or demand them in the name of keeping us safe. And then Smith tells me our lives are being recorded, he said, spelling out a simple truth of life after 9/11. It's like all these electronic diaries are being kept by different people. And then it occurred to me that we have no control over these diaries and we can't even know what they say about us.

FEMALE SPEAKER: And on that note, thank you very much.