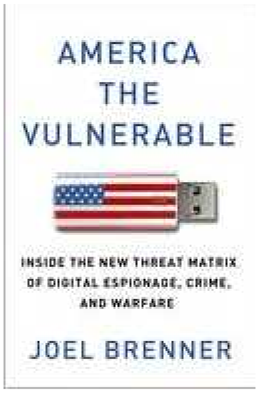
CARNEGIE COUNCIL
The Voice for Ethics in International Affairs

America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare

Joel F. Brenner , Joanne J. Myers

October 11, 2011


AMERICA
THE
VULNERABLE
INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE
JOEL BRENNER

America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare

Introduction

JOANNE MYERS: Good afternoon. I'm Joanne Myers, director of Public Affairs Programs, and, on behalf of the Carnegie Council, I'd like to thank you all for joining us.

Our speaker is Joel Brenner. For most of the first decade of the 21st century, Mr. Brenner was at the forefront of our government's efforts to thwart spying and terrorism. What he witnessed during this time as inspector general of the National Security Agency and later chief of counterintelligence for the director of National Intelligence is the subject of his book, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*.

In it he writes about a new kind of spying, one that exploits digital technology, where criminal gangs and sophisticated hackers are our adversaries. The battleground: cyberspace. This deeply concerns our guest, and after his presentation I guarantee it will concern you too.

While in the past, intelligence gathering focused on ways to improve our physical security, today our security concerns have expanded and include finding ways to safeguard our electronic infrastructure.

In *America the Vulnerable,* our speaker tells us that all is not quiet in cyberspace. If you think back to the early days of the Internet, the idea of a computer as something that could be attacked, let alone something that could be used to attack others, was simply not a consideration. Yet, in our personal life, and in the corporate and government worlds, we are facing just that—attacks in which insecure networks make privacy and secrecy nearly impossible at every level.

While you may be familiar with China's infiltration of the Defense Department, Wikileaks, or identity theft, this is only the tip of the iceberg. A new generation of spies who operate remotely from such places as China, the Middle East, Russia, and France have disabled our power plants, stolen our latest submarine technology, appropriated millions of credit card numbers, and have invaded the innermost ring of the Pentagon.

In fact, only yesterday I read about a computer virus that captures strokes on a keyboard, which infected networks used by pilots who control U.S. Air Force drones. And, according to *Wired* magazine, the spyware affecting these drones has resisted efforts to remove it.

It's no wonder the U.S. government recently decided to treat certain instances of cyber-espionage as acts of war.

Mr. Brenner writes that for years both those in the private and public sectors have known about these threats, and how vulnerable we are. Still, we are ill-prepared to stop these incursions that threaten our security. Accordingly, he argues that we can't delay any longer. Now is the time to get serious about defending our nation's secrets, wealth, and electronic infrastructure.

So how can we secure our insecure networks? For the answers, please join me in welcoming Joel Brenner to our program.

We are delighted to have you here.

Remarks

JOEL BRENNER: Thanks so much for that introduction and for the opportunity to speak to you tonight and to be here in New York, which I love.

I'm going to begin by reading from the introduction of my book to lay out some of the scope of what the issues are. Then I'm going to talk just informally about why I wrote this book, and what I've been doing that led me to want to do it. Then I'm going to give you an example of the kind of story that is in the book, about how you really blow things up with a mouse and a keyboard. So let me begin.

How did the Chinese manage to remotely download up to 20 terabytes of information from the Defense Department, equal to about 20 percent of all the data in the Library of Congress, and why don't we know what they took? And how did Wikileaks gets its hands on classified diplomatic cables, and why hasn't the government been able to shut it down? How did the specifications for the avionics and armor on the president's helicopter end up in Tehran, and what has that got to do with the theft of Supreme Court Justice Breyer's personal information from his investment advisor?

The answers to these questions reveal alarming threats to our personal, corporate, and national security that come from a new kind of espionage, and from the sudden transparency that has overwhelmed us at every level—personal, corporate, and national.

Your difficulties with electronic privacy, and mine, corporate difficulties with keeping valuable technology out of the hands of pirates, and the country's and government's difficulties in keeping secrets, have more to do with one another than you know.

I spent most of the first decade of this century at the heart of the government's effort to thwart spying and terrorism against us. Of course, in the process of that, I saw a lot of the old-fashioned kind of spying and our efforts to thwart it. But I also saw something entirely different, that spying has changed in two fundamental ways.

In the first place, if you can steal something, break into somebody's electronic system, and steal vast quantities of data—more than you could ever carry out in wheelbarrow after wheelbarrow; and you don't have to be there. If you can do that from the security of your office in Moscow or Guangdong, why do you have to run a spy? So, this is part of what has changed.

The other thing that has really changed, is that the focus of espionage is no longer virtually exclusively on the State Department, the Defense Department, the military, the White House, and so on. It's not just what we usually think of as national security secrets. The targets for espionage have now become relentlessly the intellectual property of American companies, which is what makes jobs, creates value, and makes this country really tick and turn around.

A lot of what I saw I can't discuss here—I can't discuss it anywhere—but I can tell you how this works, what the biggest and most vulnerable targets are, who does it best, as well as what it means for the future of warfare, intelligence, market competition, and our lives in general. I also came to understand what we can, and really cannot, do about it.

The truth I saw was brutal and intense. I saw electronic thieves stripping our country, our government, and our companies blind. And I'm not just talking about the pirating of DVDs in Asia of movies, or somebody ripping off your Social Security number. That stuff's bad enough. But compared to the technologies costing billions of dollars that are being bled out of our companies, this is child's play. And yet, that's fundamentally what has caught and held the public's attention, while I think we've mostly missed the slow bleeding out of what makes our country valuable.

This kind of technology is slipping out on the Internet, or it's slipping out after hours on thumb drives. You know, on a thumb drive you can now buy for a few dollars, you can put the equivalent of a million pages of documents dangling on the end of your keychain.

Remember Whittaker Chambers hiding microfilm in a hollowed-out pumpkin? Those days are finished. You could put wheelbarrows full of microfilm—all the microfilm Whittaker Chambers could have carried out in a lifetime pales in comparison to what you can put on one of those thumb drives, let alone what you can bleed out remotely, and what has been bled out remotely from our companies and our government.

This technology is reentering our country in many cases as finished products, so that in effect we end up buying back our own technology.

You know, the public easily understands that something is important when it blows up or when it's dramatic. What I'm describing to you is, apart from the capacity for some dramatic events which I'll get to, something slow. It's dangerous, and it's slow, and really important, because it involves the devaluation of the American—and indeed the whole Western—corpus of technology.

Talking about transparency, think about the Wikileaks thing, and the ability of the equivalent of anybody to catch information about critical infrastructure—dams, and chemical factories, for example—and broadcast which ones are the most vulnerable, gleefully broadcast this stuff.

You know, we can argue about or talk about when transparency is good, or when it's bad. But transparency is not an unadulterated virtue, because you cannot have unlimited amounts of transparency, and unlimited amounts of privacy or discretion. So if one treats transparency as an unadulterated virtue, then you have to regard discretion, modesty, and tact as vices, which I doubt anyone in this audience would be willing to do. The country has to think harder about this. This is a mix that we need to come to grips with.

The sudden immersion in this rapidly expanding sea of data that we love so much—I mean, we walk down the street looking at our gizmos, constantly broadcasting where we are and what we're doing. We create this sea of data. It's not being imposed on us. But this thrill that we have with it, the pleasure we get from it, and the extraordinary productivity that it has created, have also created quite dramatic vulnerabilities.

I want to explain also that one of the things that this has done to us, in ways that most don't appreciate, is that it's not only that we keep information on IT [information technology] systems. IT systems make things run. So, because of that, and because we hook up factory production, air traffic control, military technology that makes things, in an electricity grid, to the same IT systems in which we store information, it means that we've made those things vulnerable too. We have adversaries who understand this, and who are thinking every day about how to exploit that.

Electricity grids, financial systems, air traffic control—all these networks run on the same systems that we communicate on. They all run electronically, they all run on the same telecommunications background, and increasingly they all run on commercial off-the-shelf technology, which means that a high-school kid in central Asia knows how it works as well as we do.

What really sets us apart in this business is not capital. The ability to exploit these systems is not a question of capital. It doesn't take that much money. It really involves know-how, and know-how tends to level itself out, and it is leveling itself out.

You read a lot about cyber-war, are we having a cyber-war. I want to describe to you a condition of our society now, in which this transparency creates possibilities for real conflict—I'm going to describe one in a little while. But it's not, in my opinion, war.

I think the public is tired of hearing about the war of this, and the war of that, and I think we've become rightly suspicious of that kind of talk. As a matter of law, we're not at war; and, if we were, we'd really know. Some very nasty things would be happening.

But at the same time, if you talk to the people whose business it is, whose profession it is, to manage these networks for—you pick a big company; it doesn't matter which—they feel that they are being attacked 24 hours a day, seven days a week. They feel under attack.

So, this talk about war is not just somebody's attempt to overdramatize this. The probing of networks, and the attempt to penetrate corporate and governmental networks, is going on all the time, and the people who are fending this stuff off do feel under siege. There's no question about this.

What did I write this book? This is not your usual government or ex-government intelligence officer's approach to this sort of thing. I wrote it because I sat in meeting after meeting with generals and admirals, and our civilian leaders pounding the table and saying, "The public just doesn't understand what we're facing."

So I said, "I'm going to explain it." I felt that I could do this, because it has been my deep conviction, even when I was deeply in the most secret organizations in the government, that what is fundamental to understand in this area is not classified. I mean, a particular operation, the way a particular piece of code works, may be classified. But the fundamental condition that disorients us now is not a question of anything being classified.

The bits of this information are out there, but I hadn't seen anybody put it together in a way that made it clear that we're dealing with the same fundamental issue of transparency from top to bottom, or bottom to top, from personal to corporate to governmental.

Of course, you run ideas by your friends as you're writing, or when you're thinking about writing. People would say, "Is this good or bad?" My answer to that, is it's sort of like asking if gravity's good or bad. When you make policy, you have to make value judgments about what you want to try and regulate. And making value judgments of course leads to certain moral self-satisfaction—who's above engaging in that, from time to time? But it's really important to understand this is a condition of life that is in some cases good, in some cases bad, in some cases we'll argue about whether it's good or bad. But as I said before, you can't have unlimited transparency and any privacy at all, or any kind of modesty.

That brings me to another thing that I saw and wanted to talk about. Partly as a result of a number of policies of the Bush Administration, with which I'm sure everybody in this room is familiar—and I ought to say that although I served during that administration, I did not hold political office and did not want one. I was laboring in the vineyards as a career civil servant. That administration pursued relentless secrecy in many ways that I thought were profoundly unwise.

Of course, the press, which either suffers or benefits from the way the Freedom of Information Act is interpreted, has relentlessly talked about the administration's restrictive reading of that Act, kind of giving the impression that secrecy is really through the roof, while privacy is in the ditch.

The truth is, in my view, quite different: they're both in the ditch, and they're both in the ditch for the same set of technological and cultural reasons.

The government, like you or me, deals with, communicates, and operates on the same networks that we do. If those networks are porous, and subject to either being taken down or penetrated, the government is, too. In fact, we know that that has happened. It's not just large corporations that have lost their personal data, credit card numbers and such, but the government has lost, as I read, profoundly huge quantities of data to foreign spies coming remotely.

The other thing that affects our privacy, and why in my judgment it's inadequate to speak about privacy simply as to how one regulates data that has already been out of the bag—and privacy is not, after all, a subspecialty of electrical engineering. It has a lot to do with how one behaves and what information one puts out.

Looking at what privacy means in an extraordinarily exhibitionist culture raises really difficult questions of what we want to share, what we want to have, what we expect to have shared.

One hears that we're in a post-privacy or post-secrecy culture now. I think this is an exaggeration. But it really does get at a profound truth, which I'll phrase this way: Secrets, whether they're personal or organizational, are harder and harder to keep. We are, as I say in one of my chapters, electronically naked.

That doesn't mean there will be no secrets. As long as people do business together, as long as people feel any modicum of shame or guilt, people will want to keep secrets. But they're harder and harder to keep. And they will stay secret less long. I think in terms of isotopes, of a half-life of a secret. That half-life is getting shorter and shorter. Again, is that good or bad?

Well, one of the great things is it makes hypocrisy harder—that's more or less good. But, before you decide whether you think that's wonderful or not, you also need to say: "What's it doing to my life, to my children's lives? What's it doing to my ability to raise children in a way that I can control, not have the society control?"

I wanted to lay out a picture of what transparency is doing, from a personal to a governmental level.

At the governmental level, I do point out also that the intelligence business lives in the same world we live in. Transparency has come to the intelligence business.

Remember the assassination of the Hamas arms dealer in Dubai a couple of years ago? Ten years ago, let alone 50 years ago, an operation like that would have sunk like a stone. Nobody would have understood what happened. There would have been lots of rumors, guesses, but nobody would have known ever.

In that case, within 24 hours, 11 of the people on the assassination team had their photographs on the Internet along with their credentials. Within a week, all 26 members of that team had been exposed.

How did that happen? It wasn't because the Dubai police engaged in heavy-handed, Stalinist surveillance. It was because in Dubai, like in New York, everybody engages in pervasive light-handed surveillance. So the ability of the police to correlate the videos in the airport where you'd want it, and the videos in the mall—where you probably want it there too, because there's a lot less crime in the mall as a result, and the videos in the hotel—which the hotel wants because they don't want to have to deal with the legal consequences of crime on the eleventh floor, or wherever it is—the ability to correlate that information with a few clicks was extraordinary.

What it means, is the first assassination in history which is recorded in hundreds of hours on video, all but the actual murder in the hotel room. Transparency has come to the intelligence business.

Also, you think about the CIA rendition flights. How were they exposed? Not by any government. They were exposed by amateur sleuths who were plane spotters, who go out in airports and write down the numbers on the tail of an aircraft and all that sort of thing.

The European governments got into the act when that bandwagon was already rolling. You could always find out somewhere, by standing in line for a long time, or filing a written request, to find out who owned a certain aircraft. It might take you a long time to figure it out.

I could tell you now online—you could tell me, yourself, online—at certain websites who owns any aircraft in the world, and whether that tail marking has ever been changed. So the changing of a tail marking is no longer a way of disguising something; it's a way of advertising that there's something funny going on.

So transparency has come to the intelligence business. That means that cover, aliases, are real hard. When you go across a border and say, "I'm Thomas O'Hara from the Acme Metal Company," trying to get into somewhere in the Ukraine, the guy looks at his stuff and your fingerprints and says, "I know who you are. You're Joel Brenner, and here's your background. We know a lot about you. Would you step into this room over here?"

So the whole business is really, really changing. So what I've tried to do is lay out the relationship between this transparency, which starts when you give the grocer a lot of information about your purchasing habits because you want to save a buck on a bunch of grapes, down to, when you go across the Triboro Bridge, do you stay in line and pay that toll, or do you sail through on an electronic pass? You create a record of where you go. You create footprints.

You probably don't pay cash much anymore. There are a lot of people younger than most of us in the room who will use a credit card to buy a cup of coffee. The footprints that you leave behind you when you go through life like that are extraordinary and they are really detailed.

It's not the government that's amassing this stuff. It's private managers of databases who sell this information. It's happening more slowly in Europe because the rules are tougher there, but it's happening there too.

That's the sort of thing that I try to integrate, a picture that goes from the personal to the corporate to the national, in this book in ways that no one has ever done, and that I think lays out some of the national issues much more candidly and in more detail than anyone has ever done.

Let me read you a very short piece that will illustrate a point I made earlier about how it is not only do we store information on these networks, but we also use it to make things work. Then we'll open it up for a conversation.

This is the beginning of a chapter called "Dancing in the Dark." It's about the electricity grid:

> On March 4, 2007, an electricity generator from the Alaska grid began to vibrate, slowly at first, then faster and faster, until the delicately balanced turbines in the massive generator rumbled, shook furiously, and blew apart. Then the generator just shut down, hissing and belching smoke from its burned-out coupling. Explosives didn't destroy this hulk of equipment, though you might have thought so from the look of it. Nor was it employee sabotage. The saboteurs were outsiders miles away, and their tools were a keyboard and mouse. They evaded firewalls, took over the controls, and opened and closed breakers at will, all the while manipulating the operator's screen to make it appear that nothing untoward was happening.
>
> Fortunately, the generator had been removed from Alaska and carefully reconnected elsewhere so that blowing it up would not wreak havoc on the grid. It was a secret experiment carried out by clever researchers at the Idaho National Laboratory. They reportedly called their project Aurora, and they blew the turbines apart by hacking into the digital devices that regulated power on the grid. When they got into the system, they simply instructed it to make rapid changes in the electricity cycles that powered the equipment—fast, slow, fast, slow—and then they waited, just about a second or two, to wait for the thing to blow up. And it did, it exploded.
>
> Neither the United States government nor private industry can defend the networks on which our economic and national security depend. The situation is getting worse, not better. The Aurora experiment demonstrated that a risk to information technology had become a risk to operational technology. But few companies in the power-generation business were paying any attention.

> Electronic security, physical security, and operational security are no longer separate lines of work. Electronic security used to mean keeping your information secure and available, and the guys who did it were the geeks in the computer closet tinkering with racks of equipment.
>
> Physical security, on the other hand, was all about guns, gates, and guards—the flatfooted guy in rubber soles—and the guys who did that were in-house cops.Except in intelligence agencies, where operational security permeates every part of the business, operational security in most firms was just an aspect of physical security: protect the building and the people in it and you could keep doing business.
>
> Both types, the guards and the geeks, were specialized support cadres that most executives could ignore most of the time. Business executives and government officials who still think so are asking for trouble. In the old days, a burglar got into a building by throwing a brick through a window, by taking a crowbar to the door, or picking a lock; and burglar alarms made that a little bit more complicated, but not much. Today, however, your entire perimeter of windows, doors, gates, heating and ventilation, information systems, all go back to that same closet. The guys in that closet now control everything you do.
>
> If an intruder can break into the right server electronically, he can remotely shut down production, send your goods to the wrong destination, unlock your doors, shut off your HVAC (your heating, ventelation and air conditioning), or steal information and delete the log entries that show whether anybody was ever there. The company's private security guards are also electronically connected. If an intruder could get access to the chairman's calendar, planning an assault or a kidnapping becomes a great deal easier. Everything you do goes back to that computer closet.
>
> I'm afraid, however, that the people who own and operate our electricity grid still aren't paying attention.

So let's have a conversation.

JOANNE MYERS: Thank you. I'm just wondering—you talked about in the past how there was an alarm system. So what is the alarm system to warn us now that something is taking place?

JOEL BRENNER: Let's take a big company, like General Dynamics or AT&T. Those companies monitor their traffic constantly. But even they sometimes are fooled when they're subject to an attack by, let's say, a Chinese government espionage attack. We have, though, at that level—and we have it in the Defense Department—they watch their systems all the time.

In the civilian part of our government, if I said it was ragged and uneven, that would be putting it mildly.

But what we do not have is something to tell us whether there was a slow-motion attack on the country that was unrolling slowly, because we don't have the government, and don't want the government, in all of our networks all the time, do we? I don't think so. I don't.

But we don't have that kind of seamless cooperation even among the major players in the private industry.

Questions and Answers

QUESTION: Don Simmons is my name.

I have read things about encryption, some of the most sophisticated techniques of which involve large prime numbers, and so on. Are we in a state where any message, no matter how sophisticated our encryption, can be decoded?

JOEL BRENNER: No, I don't think we are.

Mr. Simmons is asking about how good is the encryption that's available and can it be broken.

Breaking the best encryption takes time, and it isn't worth most people's trouble to do it. But information—if you have a key logger on your system, the encryption doesn't do you any good.

Earlier this evening we heard about malware that was in the control system for the drones that we fly. A key logger means that some software is making a record of every keystroke that's being made. If the information that's being recorded is then subsequently encrypted, it doesn't matter, because it will have been recorded before it was encrypted.

Let me back up. Even though I can describe all these sophisticated attacks on encryption systems, most people don't encrypt most stuff. The reason we don't know what exactly the Chinese took from the Pentagon—in that event that I described at the very beginning of my remarks—is that we didn't encrypt it. The Pentagon thought it was too much trouble and expense. It was unclassified information, but very important.

There's a lot of sensitive information that's not classified. For example, if you know the identity of every person in the United States military over a period of years, you're going to also find out the identity and a lot of biographical information about a lot of people who end up going into the intelligence services later on after they get out of the military. That's very valuable information.

But we all know exactly what they took because they encrypted it on the way out the door, the electronic door. We didn't encrypt it; we thought it was too much trouble. They encrypted it while they were stealing it. I mean, you talk about sophisticated malware! So we don't know what went.

So part of the issue with encryption is making it easier and more seamless for different kinds of software to talk to one another and handle encrypted communications.

But let me bother you some more with this. When you encrypt something, let's say a communication on a cell phone, and it goes to a cell tower, it sometimes, in order to get passed on, has to get re-encrypted to be handled by the next leg of the journey. At that point it's for a fraction of a second decrypted and what's called "in the clear." So if somebody penetrates that cell tower in what's called a "man in the middle" attack for obvious reasons, they can steal it then too.

This is a game of leapfrog, of security and breaking, security and more breaking. It's just Wild West out there.

QUESTION: James Starkman. Thank you for a very frightening but interesting talk.

Using as a metaphor Wikileaks, how would you on balance evaluate morally the role that they played? And also, what do we know about the technology that they employed to do what they did?

JOEL BRENNER: Let me try to go through those questions in the reverse order, and if I miss something, you hold me to it.

What they did in terms of stealing didn't involve anything very fancy. It appears that—it's alleged and appears to be true—that Private Manning, a rather unstable guy in Iraq, downloaded a lot of information, most of which had nothing to do with his job—we should come back to that in a minute—and put it on disks, encrypted it and hid it underneath some music stuff. There was nothing fancy about that.

What made Wikileaks so survivable is that it had mirror sites in a great many countries around the world beyond the control of any government or any group of friendly governments. It had servers with the same information in many different places. So taking down one or some of these servers was pointless, as a judge in California found out when he tried to do it. There was an injunction against Wikileaks requiring them to take certain information down. They just sort of laughed.

That wasn't a fancy technology; it was a very sophisticated use of technology.

How do I evaluate the morality of it? I evaluate it in the same way that Reporters Without Borders, for example, were horrified at the release of information that disclosed the identities and put lives in danger. There's no question in my mind that many lives were put in danger. An opposition leader in Zimbabwe had to leave the country, for example. We know that in Afghanistan the names of people who were cooperating with us against the Taliban were exposed, and the Taliban made a point of saying, "We're convening a committee to go through this stuff to figure out who these people are." I think that was by any standard—of either decency or professional journalism—disgraceful.

There was also a lot of stuff in there that—we talked about transparency earlier. There were that I saw, other than the individual stuff, no individual identities, no state secrets; no big pictures were changed. What we saw was how diplomacy takes place in private. Just the way that you will speak differently to a business associate or a family member in private than you would in public, so do diplomats. They cannot speak candidly if they can't do that.

Some of the stuff that came out was really almost—lots of it was really interesting, let's face it—and some of it demonstrated the over-classification problem that we certainly do live with. That's another conversation we could have long into the night. There's a lot of over-classification. We also under-protect certain information, but we over-classify a lot. Is it good that some of that came out? It's okay. I think over-classification is a significant issue.

But again, we are dealing with the ability of some clever people who don't like us. There's no question that Assange is profoundly and deeply anti-American and anti-capitalist, deeply anti-capitalist. I don't mean just robber-baron capitalist. He's against capitalist business. I thought that was pretty awful.

But again it comes back to my comment about gravity. You know, it's there. That's not the last of it and there are already lots of imitators.

There's another aspect of it, though, that really can teach us something. I've written for the papers and magazines about why did this guy Manning have access to this information. What is a private in Afghanistan, sane or not, doing with information about private conversations with the King of Saudi Arabia or conversations about the American ambassador in Reykjavik regarding the Icelandic economy? Why do we do this?

I've had businessmen come up to me in talking about this and say, "Boy, that was stupid of the government. The government must be really dumb."

True, this was really irresponsible of the State Department. But my answer—I love it when I get the question or that statement from business people, because I look at them and say, "Tell me, why does the guy in your mail room have access to everything on your server?" I watch the guy turn white. Because it's the same problem.

In the government, we for a long time had a system of classifying information and tagging people according to their access, who can access information at different levels of classification—low level it's confidential, secret, top secret, and so on. That has been foreign to American business or Western business in general, except in the M&A business you've got to keep the trading desk—the trading desk has got to be really carefully kept apart from the M&A boys, and you say you have a Chinese wall, so-called. And quarterly financial stuff is guarded carefully within firms.

But except for certain things like that, by and large most businesses have an information system, and if you have access to any part of it, you have access to all of it. It's sort of like an M&M [candy]—it's supposedly hard outside and it's real soft in the middle. You can go anywhere with it.

That's starting to change. Businesses are now going to what they'll call "role-based access to information"—in my opinion not fast enough, as I say to some of my clients.

It's, again, why does the guy in the mail room have access to your engineering drawings? He doesn't need them. Why does he have access to a lot of your financial data or to everything on your mail server? Why does the guy who has access to the financial data but isn't an engineer have access to the other stuff?

So businesses are starting to realize that if they want to protect certain information, if they want to lengthen the half-life of the things that really make that business valuable, they have to start thinking about who gets to look at what. We're not too good at that.

QUESTION: Hi. I'm George Janis, and I'm very interested in the prophecy.

I think we all agree, at least in this room and in New York, that the financial trading system is the heart of our capitalistic system. Are you saying in your book, or predicting in your book, that its destruction is not a matter of if but when?

The second part of my question is the meltdown that happened last year in the New York Stock Exchange, where the government has never really explained what happened. Do you believe that was the result of hacking?

JOEL BRENNER: The flash crash, you're talking about. I don't know. I don't want to engage in speculating about that for the sake of a dramatic answer to your question. It's a good question. I think probably not. Let's put it this way. There's no evidence that it was a result of hacking. It could have been.

But just like the blackout in San Diego a month or so ago that lasted about a few hours, what can be done accidentally can be recreated on purpose.

I'm not predicting the imminent demise of the trading system. No, I'm not. I think we've got much more likely things to worry about in terms of the economy or the stock market than that.

It is not beyond conceiving, however, that you could imagine a brokerage house being hacked and some weird trades being put in, or just tinkering with prices. I mean, if somebody really was just malicious and mischievous, almost worse than bringing a system down is corrupting the data in it.

Imagine what the clearing process is going to be like at the end of the day. The boys in lower Manhattan will really stay up all night and they'll have to unwind a lot of trades. Then you want to speculate, could it be so complicated that they couldn't unwind some of those trades? Possibly. That system actually is more robust than the systems in most American businesses.

But we do see now—I haven't had a chance to read it, but I saw it flash across my screen late today, the thought that Anonymous [Hackers Group] might have slowed down some of the trading on the New York today. I haven't evaluated that yet.

What they do is sort of juvenile delinquency. It's called a DDoS attack. It's a distributed denial of service attack, which means flooding somebody's servers with so many communications in such a short period of time that they just basically collapse.

We're pretty good at knowing how to shunt that stuff into a black hole. It's not a very sophisticated form of disruption. I'm pretty sure that the exchanges will deal pretty well with that sort of thing.

The corruption of data or the placement of trades designed to manipulate the market, as you described, I think that's a more serious danger. But I don't see it as bringing down the market, no.

QUESTION: David Hunt. I worked for the CIA for many years as an operations officer.

In the early 1990s, I represented the Operations Directorate and a CIA task force to fend off requests by the White House and the new Clinton Administration to open up all our secrets because they wanted transparency. They could not understand really the whole purposes of security clearances or polygraphs. They railed against us. They said, "There's no reason in the world why anybody in the government should not be able to walk into CIA headquarters and learn what's going on."

I would submit that the Wikileaks was a result of DoD [Department of Defense] and State [Department] basically succumbing to that philosophy that, yes, everything can be open.

But it's certainly wrong when an American ambassador in, say, Pakistan or Afghanistan has a private conversation with Karzai, and it's all over the place. That's just wrong. We just refused to do it. You will not find any CIA operational stuff—maybe some finished intelligence—on the whole Wikileaks network.

My question to you is: Can DoD or State really begin to pull this back in now, so that they can control it in a more effective way so that this will not happen again?

JOEL BRENNER: You know, Mr. Hunt, you and I have worked in profoundly secret, powerful organizations created in a democratic republic that profoundly distrusts power and secrecy. So let's talk about that problem before we come to the tactical issues that you've put on the table. That's the strategic issue as I see it. I think it underlaid the great debate and anger over the surveillance program and the way that that was done during the Bush Administration.

Almost everybody, except at the extreme fringes, will acknowledge we need intelligence services. But these services are secret and powerful. In my view, secrecy is like power, and to paraphrase Lord Acton, secrecy corrupts and absolute secrecy corrupts absolutely.

The only way we square this circle in a democracy is by creating oversight mechanisms that really are meaningful. That was what the Congress tried to do in 1976.

The Congress doesn't do anything with a scalpel. When it finally gets energized, it uses a bludgeon or a meat axe. That's the only way that a legislature can approach a problem like this. So they created the FISA Court [Foreign Intelligence Surveillance Court], and that sort of thing.

From time to time, periodically, we will as a republic have to look at the adequacy of these mechanisms to supervise the kinds of organizations you and I have worked in, because left to their own devices they will get off the rails because secrecy corrupts.

The difficulty is: What kind of transparency do you want in these organizations? You can create, for example, a FISA Court, the Foreign Intelligence Surveillance Court, but it has to do things in secret too. So what you have to do is create mechanisms that you can have confidence in, even though the public just can't look at everything that is going on in that tent. That's to me the strategic issue.

The Clinton Administration, which I in many respects thought was a good time for the country, really started out not understanding this very well at all and proposing some nutty things.

Of course, over there in Langley [location of CIA headquarters] you guys are really good at dragging your heels and knuckles and everything and keeping that stuff from happening. So you kept that pretty well from getting out of control.

Wikileaks, as I said, is going to happen again. This is imperfect. We can't think in terms of locking this stuff up. This country's great not because it's secret but because it's open, dynamic, and it moves fast, which is why speed, not secrecy, is increasingly going to be the coin of the realm.

You know, we can get better at this, you can reduce the likelihood of the sort of Wikileaks thing. As I say, I think that was not only predictable, I predicted, not that it was going to be Wikileaks, but that sort of thing was going to happen. But things like that are going to happen again. Transparency is in the business now, and it's even in the business at Langley and Fort Meade.

QUESTION: My name is Mike Smith. I work with the UN on counterterrorism.

There was something I find a bit intriguing here. You were describing a situation where personal information on all of us is out there. It's collected in some places by different bodies. Most of it we don't seem to worry about, maybe because we don't fully appreciate the extent of it. But one thing is very clear, that in our societies—I come from Australia, but I know in Australia it's as bad as here, or as good, in the sense that people are quite allergic to the idea that the government should have this sort of information about people and should gather that information.

Now, after 9/11 here, through Homeland Security, a system was set up to record data on every foreigner arriving in this country. So people get their pictures taken, their fingerprints, at the airport on their arrival, or at a port. It doesn't apply to American citizens for obvious reasons. It would be completely unacceptable.

Interestingly, though, that same technology has been spread by the United States to many other countries. So when Americans do turn up in Pakistan or places, they are being photographed and fingerprinted. That data, I don't know quite where it goes other than to the local authorities, but it may go further.

I guess what I'm saying is should we really be worried about this, because in the long term—you gave a very good example of you pretending to be someone else turning up at the Ukrainian border and being spotted. In my game, one of the things that is positive about the way in which we can now gather detailed information is that it's much more difficult for terrorists to cross borders, because it's very difficult to forge ID documents when you have biodata included on them, et cetera. On the other hand, it is an invasion of our privacy.

Where do you think we go with all of that?

JOEL BRENNER: I think it's more than an invasion of privacy. I don't think you can go through an airport in the United States, or in any industrial country now, without suffering what I think on any reasonably account are just extraordinary indignities. But if you say that to most people, especially younger people, they don't know what you're talking about.

Privacy is, after all, a matter of dignity. It's not just a matter of deciding who gets what—I'm going to put this out there and you can have it, you can have it, and you can have it, but he can't. Those rules are very difficult to deal with. We should be worried about this.

But let's back up. It's really important to keep in mind in my view that most of the research on data and most of the aggregation of what people in the business call "big data" is not being done by the government. There was a piece in *The New York Times* yesterday or today about IARPA [Intelligence Advanced Research Projects Activity] doing things like that. The government is doing all kinds of research, and should be doing research, into this, because if they're not understanding how to put the data together, somebody else is understanding how to put the data together.

But most of the information that is out there is given away. You know, data is very powerful, hugely powerful, a predictive tool for good and ill. I wonder whether in 40 or 50 years or 100 years people won't look back at our attempts to decide who can use data for what, like Medieval attempts by the church to control who could have access to certain information, or what information was inherently bad or should not be learned, should not be looked into. I'm not predicting that, but I scratch my head and I wonder about that.

Now, it's important to remember, though, that data—look, the government can tax us and put us in jail. That makes them different from the grocery store. That's why controlling what the government can learn about us and the procedures that they have to go through in order to do it is really, really important.

For example, right now one of the significant issues before the federal courts at the appellate level is when the police need a warrant to require information about geolocation—where you are. There's lots of information about geolocation.

When you use one of these things [points to cell phone], you're broadcasting this stuff. If it's got GPS [Global Positioning System] in it, it's very precise. If it doesn't have GPS, it's within a couple of blocks or a block or two because you triangulate from these cell towers, like you learned to do in geometry in the tenth grade.

We have some real difficult legal issues about how to handle this. But the courts are coming in the direction that I like, which is that if this is persistent, if this is not just one trip, if you're really following somebody around for a significant period of time or following them into their house, you need a warrant even though the statute doesn't require it.

I think these are terribly important. But again, the data is out there. I don't think that toothpaste gets put back in the tube.

Now, you mentioned a couple of other things too, including the uses of technology when they're exported. Technology for good can also be used for ill.

There's a real problem. You remember perhaps the question in the mid-1990s about whether we in the United States were going to allow serious cryptography to be exported. We didn't want to do it because if our adversaries, and even some of our friends, could encrypt their communications to a high degree, we couldn't read it anymore.

Then we realized that gosh, if the rest of the world weren't using our cryptography, they'd be using French cryptography or Israeli cryptography or Russian cryptography. So we might as well sell it out there, because if we're going to break something, we might as well try to break our own stuff because we know how it works. And we want American businesses to capture this world market, not the French, the Israelis, or the Russians.

The urge to regulate this sort of thing often assumes that the technology being regulated is static, and it never is. I think the problem comes up now in exactly the same way with technology that could be used in court-supervised ways that are perfectly acceptable in this country, but the Chinese, for example—not just them; Chinese, Zimbabweans, Russians, pick your favorite bellwether of liberty—use in ways that horrify us.

But because we don't like it, and even because we say, "Holy mackerel, that's a Cisco router they're using that with, that's an American company," that doesn't mean we can regulate it. The attempt to regulate it often runs us into unintended consequences.

This is a very bad problem, but I don't know that it has a solution.

JOANNE MYERS: Well, now that you have upset us all, I'd like to invite the rest of you to come and continue the conversation.

I thank you for a very interesting talk.