

Corporate Responsibility in the Information Age

TRACK DESCRIPTION

WatchIT.com™; brings together the best in IT. Our monthly program features technology experts, business leaders and industry analysts who offer a comprehensive perspective on the trends, issues and technologies important to today's IT professionals. Understanding, advice, best practices: you get all of this and more from WatchIT.com™.

In partnership with leading experts, analysts and consultants, the Guest Track is designed to provide viewers with a head start in crafting and deploying management and technology strategies that strengthen competitive advantage.

INTRODUCTION

Hi, I'm Barry Steinhardt. I'm the associate director of the American Civil Liberties Union, and chair of our privacy task force. In the interest of full disclosure, I should also tell you that, yes, I'm a lawyer.

Welcome to this WatchIT.com™; Guest Track program, Corporate Responsibility in the Information Age.

AGENDA

Let me begin by setting the agenda.

- ~ First, let's talk about privacy invasions: fantasy or reality?
- ~ Then, let's talk concretely about how technology has threatened our privacy. We'll look at some actual examples;
- ~ After that, let's talk about the public and political realities about regulation and privacy;
- ~ Then the basic fair information principles;
- ~ Then I hope to give you some general recommendations for business responsibility in this area – recommendations that come from the business community itself;
- ~ Then we can turn to two real examples of how industry can respond to privacy concerns;
- ~ Finally, let's talk about the government: how it is part of the solution, but also part of the problem.

ROI

By watching this program, we hope you'll have a better sense of corporate responsibility in the Information Age.

We think that privacy makes good business sense, and that it makes good business sense to assume responsibility.

Some of that responsibility may well be imposed upon you by the government.

PRIVACY INVASIONS: FANTASY OR REALITY?

Let's begin with privacy invasions: fantasy or reality? Here's a scene from the future – although the not too distant future, I think:

Sally Jones is window-shopping. She is walking down any Main Street in the USA. She briefly glances at a red sweater in the window. Suddenly, her cell phone rings. A solicitor is there who wants to know if she's interested in buying that red sweater to go with the black skirt that she bought last month.

I want you to think about whether or not this is fantasy or reality.

A highly decorated soldier has an AOL screen name, a pseudonym. That screen name suggests he may be gay. He posts something on AOL, again giving a hint that he may be gay.

The wife of one of his fellow officers sees it and contacts Naval Intelligence. A Naval Intelligence officer – in violation of the military's "Don't ask, don't tell,..." and the part that's often forgotten, "...don't pursue," policy, that bars inquiries into a soldier's or sailor's sexual orientation by using a subterfuge – obtains his real name from AOL.

Discharge proceedings begin.

Fantasy or recent reality?

That story is true. It happened to a sailor with the double misfortune of being named Timothy McVeigh. Not the Timothy McVeigh of the Oklahoma bombing, but just a good sailor named Timothy McVeigh.

McVeigh sued the military and AOL. He won, but his life was ruined.

HOW TECHNOLOGY HAS THREATENED PRIVACY

The question then is: How has technology threatened privacy?

You know the public, press and government are fascinated with Internet privacy. They should be. The Internet raises very significant privacy concerns. But Internet privacy is just the tip of the iceberg.

Technology has created a host of new privacy issues – issues that the business community and the government have a responsibility to address.

Data Was Unorganized and Hard to Locate in the Past

There was a time not so long ago when data could only be found in paper form in clerk's offices.

The data was difficult to find, and it was often buried somewhere in a cubbyhole. Databases, if they could be called that, were virtually impossible to correlate.

Those days are over.

Has Easy Access Given Data Greater Value?

Powerful data collection technologies and distributed networks like the Internet have changed everything.

Collections of data that were once dispersed in those cubbyholes now reside in databases that are both comprehensive and instantly cross-accessible.

The speed and ease of correlation have given value – or, at least, perceived value – to previously worthless information.

Individuals Provide Private Data Every Day

Every day, ordinary people give away private data, from sensitive medical information, to Social Security numbers – which are the key to identity theft in this country – to all sorts of financial information, and every other imaginable piece of information about our daily lives.

Often, we provide these facts without understanding the consequences until it is too late. Every day, new technologies threaten to create what amounts to a surveillance society.

Olmstead vs. the United States

Let's look back to 1927.

Robert Olmstead was a bootlegger who sold illegal liquor during Prohibition. Today, I suppose he'd be called a liquor wholesaler. He would be president of the local Rotary Club. But in those days he was considered a criminal.

He was convicted based on what we would think of today as a primitive wiretap. That was the first wiretapping case to reach the United States Supreme Court, known as *Olmstead vs. the United States*, back in 1927.

At that time, the Supreme Court ruled that a wiretap was not a search under the Fourth Amendment, which protects us against the government's invasion of our home and our property without a warrant or probable cause.

That 1927 decision was ultimately overturned by the Supreme Court in 1967, in a case called *Katz vs. the United States*, where the Supreme Court recognized that you could violate the

Fourth Amendment even if you don't physically enter someone's home. They decided that a wiretap was a form of a search.

Justice Louis Brandeis, who is best known as the father of modern concepts of privacy, wrote the famous dissent (in *Olmstead*) in which he said, "The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping."

Justice Brandeis could not have imagined how right he was about the progress of science.

New Technologies Enable Big Brother

Indeed, if he had written that decision in 1937 or 1967 – or perhaps even 1997 – he could not have imagined the technologies that we now have, and soon will have, that enable not only the government, but private industry, to monitor our daily activities, our conversations, our movements, and our preferences.

All that is now possible with modern technology.

CONCRETE EXAMPLES OF PRIVACY INVASIONS

Let's return to the concrete examples.

We have Sally Jones, who you may remember from our first scene is window shopping on Main Street, USA. She sees a red sweater in the window. Her cell phone rings. A caller wants to know if she wants to buy the sweater to go with last month's black skirt.

Let's talk about two very real scenarios under which this can happen.

Tracking a Cell Phone's Location

The first involves the use of location tracking.

Sally's cell phone is capable of revealing her location. The store is notified that she's in the vicinity and given her cell phone number. Her records are checked and the caller is told about her past purchases.

Biometrics

Let's look at a second way in which this can happen, through the use of biometrics and video surveillance.

Sally's image is captured by a video surveillance camera. The store uses facial character recognition technology to compare her image with a photographic database – in this case, let's say credit card holders. Her records are checked. The store learns not only her cell phone number, but also learns about her past purchases. Just add a little extra. Let's imagine that the solicitor is told that she seemed particularly excited by the red sweater. How did he know that?

IBM's BlueEyes

Well, one way he can know that is with BlueEyes from IBM.

According to IBM's Web pages, BlueEyes is a sensing technology that uses video cameras and microphones to identify and observe a user's action to extract information, such as whether the user is looking intently, and what the user is saying, verbally and with her gestures.

These cues are analyzed using sophisticated algorithms to determine the user's physical, emotional or informational state. At least that's what IBM says that BlueEyes can do.

PUBLIC AND POLITICAL REALITIES ABOUT PRIVACY REGULATION

Now, what are the public and political realities about privacy regulation?

Scott McNealy, who is the CEO of Sun Microsystems, said, in a moment which I suspect he would like to have back, "There is no more privacy. Get over it."

He may claim that privacy is dead, but I don't think so. It's clearly on life support, however – and the public is demanding heroic measures to save it.

The Public's Cry for Privacy

We can see that in political action.

Just recently, 35,000 people sent faxes to the Health and Human Services secretary Tommy Thompson, demanding immediate implementation of medical privacy rules.

More than 200,000 e-mails were sent to the Federal Reserve, opposing the so-called "know your customer" bank surveillance rules that would have required all the nation's banks to create dossiers on their customers and turn that information over to a federal financial center.

We also see it in widely reported polling data.

In a Business Week/Harris Poll in March, 2000, 68% of Internet users "would not at all be comfortable" if a Web site were to merge their browsing and shopping habits into an individual profile linked to their names.

Eighty-two percent of Internet users "would not at all be comfortable" if a Web site merged, not just browsing and shopping habits, but such information as income, credit data, medical status or driver's license numbers.

Again, in the Business Week/Harris Poll from March, 2000, 57% of consumers want laws regulating the collection and use of personal information, and 41% of those who make purchases online are very concerned about the misuse of their personal information.

Business is also beginning to see this concern about privacy in the bottom line. The dot-com world is much like the miner's canary: it's the first to show the effects, but it won't be the last.

The Bottom Line

Let's talk about the bottom line.

Forrester Research found that 45% of consumers do not currently make purchases online, but would do so if their privacy concerns were addressed. Fifty-two percent of current buyers would make more purchases if they felt that their privacy concerns were being addressed.

It hits revenue. Forrester also estimates that \$12.4 billion in e-commerce sales were lost in 2000 because of privacy fears that drove consumers away from the Internet.

The Bottom Line: DoubleClick

Famously, the share price of one publicly traded banner ad firm, DoubleClick, dropped by half in the wake of negative publicity surrounding its attempts to merge online and offline data.

A year later, the share price was still down significantly.

BASIC FAIR INFORMATION PRINCIPLES

What does the public want?

I think what the public wants are the basic fair information principles – basic common sense, fair information principles.

Those fair information principles have been around for a long time. They've been recognized by governments, both here in the United States and around the world.

Basic Fair Information Principles: Limitations on Collecting Personal Data

A good example comes from the United States Department of Health, Education and Welfare – the predecessor to Tommy Thompson's HHS. They looked at these principles back in 1973.

The first is collection limitations.

There should be no personal data systems that are created – no data that's collected – whose existence is secret.

Basic Fair Information Principles: Disclosure and Secondary Usage

The second is disclosure.

There must be a way for an individual to find out what information about him is being recorded and how it's being used.

The third is secondary usage.

There must be a way for an individual to prevent information about her that is obtained for one purpose from being used or made available for other purposes without her consent.

Basic Fair Information Principles: Record Correction and Security

The fourth is the question of record correction.

There should be a way for individuals to correct or amend their record if identifiable information about them is wrong. It happens all too commonly.

Fifth is security. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of that data for their intended use, and must take precautions to prevent misuse of this data.

HOW TECHNOLOGY HAS THREATENED PRIVACY

What should industry's response be?

I think industry would do well to follow the recommendations of Business for Social Responsibility.

They made a number of common sense suggestions.

Common Sense Privacy Recommendations for Business

First, business should acknowledge that customers own their own personal information.

Second, businesses should collect and keep only that information which they will actually need. They should not collect information just because they can.

Third, businesses should seriously consider opt-in as a business model. Consumers should be given the choice to opt-in to data sharing, rather than simply the choice to opt-out.

This can provide you with a marketing advantage by establishing good will. It will make it more likely that customers will give you accurate information, and won't provide you with false information in order to avoid invasions of their privacy – and the very kind of record-keeping that you may think is of value to you.

Consider:

- ~ Appointing a privacy advisory board;
- ~ Hiring a Chief Privacy Officer (CPO); and
- ~ Conducting external privacy audits.

You should appoint a privacy advisory board with at least some independent members from outside your company, and a Chief Privacy Officer who has direct access to senior management.

It's also essential to create strong data security systems. The most serious and overlooked areas of risk to companies are probably from internal information and management errors.

Train Personnel on Privacy Policy

Remember the story of Timothy McVeigh, the sailor.

America Online actually had a policy that prevented the very disclosure of the information which they illegally disclosed to the Navy, and which the Navy illegally sought.

The problem was that their personnel weren't trained very well, and disclosed it anyway.

Design Privacy Into Your Product

You should also think about designing privacy into your products.

When you're writing code and creating services, build it right in. It's much simpler and more effective than trying to retrofit it into an architecture that's not meant to support it.

There are a lot of companies out there that can help you find the right way to build privacy into your products.

One you may want to take a look at is Zero-Knowledge Corporation. You can find them at zeroknowledge.com, but there are many others that you might want to take a look at.

TWO EXAMPLES OF HOW INDUSTRY CAN RESPOND TO PRIVACY CONCERNS

Let me give you two examples of how industry can respond to privacy concerns.

The FCC has mandated that location tracking be built into cellular networks for use by emergency services workers. So, if you have someone injured in an automobile accident, unable to use the phone, their cellular phone can be used in what is known as E911 (Enhanced 911) to identify their location.

That's a good use of the technology.

The Battle Over Location Tracking

But both law enforcement and private enterprise want access to that same information – which was created for purposes that require use by emergency services workers.

The cellular industry has responded to this call from other industries and law enforcement by petitioning the Federal Communications Commission to implement rules that rest on those fair information principles – especially notice and consent.

Again, it's the cellular industry itself that is taking the initiative and has filed a petition with the FCC.

The Battle Over Location Tracking: Notice

Here's what they ask for:

Notice: first and foremost, they ask that location service providers be required to inform the consumer about specific location information collection and use practices before any disclosure is made of personal information.

The Battle Over Location Tracking: Consent

They also ask that we have opt-in consent.

The hallmark of the CTIA privacy principles is the requirement for express authorization prior to collection activity: opt in, not opt-out – express authorization, express consent.

The Battle Over Location Tracking: Security and Integrity

Then they've asked for security and integrity.

They recognize that location services providers should maintain any information in a secure way. The systems employed by those services should provide that the location information is protected from both unauthorized access and disclosures to third parties that are improper.

The Battle Over Location Tracking: Technology-Neutral Principles

Importantly, they've also asked for technology-neutral principles.

They've said that neither a company's privacy practices nor, importantly, a consumer's privacy expectations, should be determined by the nature of the location technology.

It's an extremely important point when you think about it. Technology changes all the time. We need to have rules to cover technology and the collection of data – particularly sensitive data like our location.

What they've said is that location-based services should be technology-neutral.

Privacy standards employed should be the same whether the service is a handset – the cellular phone that we are all familiar with – or is network-based.

Privacy Practices for Biometric Devices

Similar practices are being proposed for the use of biometrics technologies like facial recognition systems, the kind that were used in my example of Sally Jones.

Let me talk a moment about the recommendations of the Bio-Privacy Initiative.

The first thing they suggest is that we draw a distinction between verification and identification.

Privacy Practices for Biometric Devices: Verification vs. Identification

A system that is capable of performing one-to-many searches – like the one used in my example of Sally Jones, where her image was compared to, perhaps, millions of others – is far more susceptible to privacy-related abuses than a one-to-one system.

In a one-to-one system you might go into a store, or go to an ATM machine, present your ATM card, and have your identity checked against a chip on your card that contains that biometric.

Privacy Practices for Biometric Devices: Overt vs. Covert

Then there is the issue of overt vs. covert.

Systems that make users aware that biometric data is being collected and used, and that keep acquisition devices in plain view, are less privacy invasive than surreptitious deployments.

User consent is the key principle for privacy-sympathetic deployment. It's difficult to consent to covert systems.

Privacy Practices for Biometric Devices: Local vs. Central Storage

Then there is the issue of local storage vs. central storage.

A biometric system that stores information centrally in a big database is clearly more capable of being abused. Information is more likely to be used for unrelated purposes.

It's more likely to be sold off or misused than a system that involves local storage – which means storing that biometric information on the user's PC, or even on a smart card.

The location of that biometric information – the so-called template storage, in this case – is crucial. That location, whenever possible, should be local. It should be under the user's control.

Privacy Practices for Biometric Devices: Opt-In vs. Mandatory

Then, of course, there's the issue of opt-in vs. mandatory.

A biometric system, like any system in which enrollment is mandated, is far more invasive of privacy than one in which the individual can consent to the collection of their information.

Mandatory systems come under more suspicion as they are being imposed.

The users are much more likely to oppose using them – to get involved in a system like that and provide the information.

The Bio-Privacy Initiative says that appropriate protections for use of mandatory and opt-in systems must be developed.

The Need for Privacy Regulations

I think, in the end, it's important that business support common sense regulations to create a baseline of privacy protections.

The examples that I just gave you from the Bio- Privacy Initiative were examples of what they call best practices. But the truth is, we've got to go beyond best practices – we need to have laws.

Privacy Regulation Is Good for Business

Why do we need to have government regulations?

First, it's going to make good business sense in the end. Let's read this, from the petition of the Cellular Telecommunications Industry that I talked about earlier.

They said that while all these applications and services promise a wealth of consumer benefits, legitimate privacy concerns abound over fears of location-based applications that allow service providers to track where users are and send them alerts about sales or travel or personal goods.

They went on to say that the CTIA, the industry itself, strongly believes that privacy concerns regarding location information must be addressed if new services and applications are to be accepted by the consumers.

In other words, the industry needs a baseline of privacy protections if it's going to grow and these services are going to be used by their customers.

Self-Regulation vs. Legislation

So, it's the right thing to do, on those merits: to enact into law a baseline of privacy rights.

Indeed, self-regulation cannot always be the answer. Now, self-regulation has its place – especially where there is the creation of clear, prominent and comprehensive privacy policies that are verified by a third party. Those offer consumers both information and a degree of protection.

The Problems With Self-Regulation

Self-regulation has a place, but it's not the only answer.

Markets are erratic. Companies change. Priorities change. Self-regulation has not been widely embraced by the industry.

There are a lot of privacy policies out there, but very few of them contain enforceable principles of the kind that we discussed earlier.

Self-regulation certainly does not provide users with mechanisms for private redress or government intervention. In some respects, it's nothing more than a simple statement of intent.

Perhaps most importantly, some data is far more sensitive than others. The protection of sensitive information cannot be left up to the vagaries of the marketplace.

We can't have the use of our medical records, or financial information, or Social Security numbers decided by the market. We need to have that baseline of privacy protections that come to us from the government.

Information is too sensitive to leave out there to be used and misused.

Posting Privacy Policies

It's also true, I think, to say that mere notice is not enough.

There has been a lot of discussion in the dot-com world about privacy policies – about posting them online and what should be covered in them.

But if you read most of those privacy policies, the truth is that there is not much in them. Very few promises are being made, in part because companies are fearful that if they make a promise and then break it, they're going to be held liable.

Congressman Ed Markey, who looked at a lot of those privacy policies, likened most privacy notices to a burglar who comes into your home and steals your television set, but leaves you a very nice, detailed note explaining what he intends to do with that television set.

Mere notice is not enough

GOVERNMENT: PART OF THE SOLUTION, PART OF THE PROBLEM

Now, while government is part of the solution to the privacy problem, it's also part of the problem itself.

From the perspective of industry, I urge you to beware of government demands for technical assistance.

CALEA and Carnivore

Let me tell you about CALEA and Carnivore.

CALEA was the Communications Assistance to Law Enforcement Act.

It is a 1994 law mandating that modern telecommunications networks be built to be wiretap ready – the first time in our history that an industry was told that it had to build its infrastructure to guarantee the government's ability to conduct surveillance.

The Communications Assistance to Law Enforcement Act

It's a little like telling the home building industry that they have to build a peephole into every new home with the understanding that only the government would look through the peephole.

Now, CALEA was a bad deal for privacy, but it was also a bad deal for business.

When the telephone companies agreed back in 1994 to CALEA, they were promised \$500 million to retrofit their old networks. They've subsequently found out that the real cost will be in the billions.

At the time, the FBI claimed it was only interested in preserving "existing capabilities," but it has since sought a punch list of new capabilities that the industry and privacy communities have fought against for years now with expensive litigation – litigation that is still not concluded.

The FBI simply broke its promise. We shouldn't accept those promises as ironclad.

Carnivore

Carnivore: a very ominous name; I didn't make it up, the FBI did.

What is it?

It's a black box – hardware and software – attached to an Internet service provider's (ISP) network by the FBI through which all communications can flow. The FBI itself decides what information it's going to look at.

Now the FBI's position is, "We'll only look at that information which we're entitled to under law."

Essentially they're saying, "Trust us. We are the government," or in some cases, "Trust us. We are the government's spies."

Now we have a lot of reason – especially given recent developments (prior to August, 2001) – not to trust the FBI. We know that they make mistakes and hide information.

We only have to turn to the case of the other Timothy McVeigh, the Oklahoma bomber, to learn that the FBI either lost or suppressed thousands of records in that case.

So, "Trust us, we're the government," isn't a very good answer to the privacy concerns that have been raised.

What's Bad for Privacy Can Be Bad for Business

It's a bad deal for privacy to open up networks to the FBI in this unsupervised way.

It's a little like giving the FBI the authority to go to the post office and open up all the mail with the promise that they will only look at the small percentage that they have a court order for.

So, it's a bad deal for privacy. But it also turns out to be a bad deal for industry. Much of industry has opposed it.

Why?

First, industry ceded control: the FBI gains unfettered access to its networks.

Second, you run the very real risk of severe disruption.

In the only case that's been publicly discussed, we know that Carnivore was attached to the network of Internet service provider Earthlink.

You know what happened? The network crashed. Carnivore didn't work.

Finally, you're going to lose consumer confidence.

I know from talking to people in the industry that they're very concerned about all the publicity around Carnivore.

They believe, correctly so, that their customers are worried that communicating over the Internet is going to subject them to government surveillance.

For all those reasons, Carnivore has been a bad deal – not only for privacy, but for industry, too.

SUMMARY

So what are the lessons here?

I think the first lesson is that consumers want privacy.

They want to know that information will not be collected from them without their consent. That it won't be used for different purposes without their consent. They want to know, that it won't be misused.

They especially want sensitive data protected:

- ~ Financial data;
- ~ Medical data;
- ~ Social Security numbers;
- ~ Location information;
- ~ Communications information.

It's extremely important to consumers.

It seems to me that it's common sense for industry to incorporate the basic fair information principles into their practices and into their products.

It's also common sense for you to work with a privacy community to craft a set – a baseline – of privacy rights that can be built into law. These are rules that you can live with, and that consumers can live with, that establish the rules of the game. These rules will make consumers comfortable using the very products and services that you want to sell them.

I think it's also common sense for you to be wary when the government says, "Help us, help us," as if you were the police. "Help us to conduct law enforcement activities. Help us to conduct surveillance."

It's not only bad public policy, it's also bad for business, as Carnivore and CALEA taught us.

FOR ADDITIONAL INFORMATION

Once again, I'm Barry Steinhardt. Thanks for watching this WatchIT.com™; Guest Track program, Corporate Responsibility in the Information Age.

If you have any questions or comments, please contact me at: experts@watchit.com.