State Legislation and Identity Theft

Shannon Callahan

Follow this and additional works at: http://commons.pacificu.edu/inter05

Recommended Citation
State Legislation and Identity Theft

Rights
Terms of use for work posted in CommonKnowledge.

This article is available at CommonKnowledge: http://commons.pacificu.edu/inter05/47
Feature: State Legislation and Identity Theft

Posted on December 1, 2005 by Editor

Speaker Shannon Callahan

Jeffrey Barlow
Good afternoon. I’m Jeffrey Barlow, director of the Berglund Center for Internet Studies at Pacific University. Welcome to the Berglund Roundtable series. Our speaker today will be Shannon Callahan who will be speaking on the issue, State Legislation and Identity Theft. At this point let me introduce Dean Eva Crebs of Pacific University, who’s the perfect person to introduce Shannon because Eva herself, is both a PHD and an attorney.

Eva Crebs
Thank you, Thank you. The issue of identity theft is indeed a real issue for people here on Pacific, so we’re delighted to have Shannon as an expert to come and speak to us. There have been students who literally have come forward to say that they have been rudely alerted to mismanaged credit card accounts only to find out that they never subscribed for those accounts. And even today on our own internal news agency, there is an article about Internet piracy and resume privacy telling students how to guard against that particular kind of theft. So, it is a real pleasure for me to introduce Shannon Callahan. Shannon is responsible for research and advocacy on behalf of consumers in the marketplace. She testifies before the legislature and state agencies on identity theft prevention, and a range of other consumer protection and healthcare issues. She serves on the Insurance Division Advisory Committee of the Oregon Department of Business & Consumer Services. She’s a member of the Oregon State Bar, having earned her J.D. from Lewis & Clark School of Law. And she has experience here in Oregon on a range of local and statewide policymaking and grassroots campaigns and has studied a variety of state-level approaches to the problem of identity theft. So, Shannon Callahan, you are welcome. Thank you.

Shannon Callahan
Thank you. Good afternoon, my name is Shannon Callahan and I am a staff attorney for the Oregon State Public Internet Research Group, OSPIRG. First of all, I wanted to thank Dr. Barlow
of Pacific University and the Berglund Center for Internet Studies for giving me the opportunity to speak with you today. For those of you who may be unfamiliar with OSPIRG, we’re a non-profit, non-partisan public interest advocacy group with over 33,000 citizen members in the state of Oregon. We advocate on such issues as consumer and environmental protection. As the staff attorney for OSPIRG, I work exclusively on consumer protection issues, as mentioned including insurance, predatory lending, consumer privacy, and identity theft. My position entails, conducting research into industry practices, crafting and evaluating legislation, as well as advocating in the Oregon legislature.

Today, I’m here to speak to you about the identity theft epidemic and what states can do, particularly the state of Oregon can do to protect its citizens from this devastating crime. As William Shakespeare wrote in Othello, “Who steals my purse, steals trash, but he who filches from me my good name, robs me of that which not enriches him, and makes me poor indeed.” Obviously, Mr. Shakespeare understood that, one of the most valuable things we have, as an individual is our good name. And 400 years later, it is individuals’ good names, their financial security, their time, and much more that the crime of identity theft takes from consumers. In a nutshell, identity theft or I.D. theft as it’s commonly known, occurs when someone uses your personal information without your permission to commit fraud or other crimes. However, how the thief gains access to your personal information and how they use that information varies widely.

While the entire nation is in the midsts of an identity theft epidemic, in fact, 10 million new victims from the United States will be victimized just this year alone. The problem is actually, particularly acute here in Oregon. In fact, the federal trade commission, the FTC, ranks Oregon as the 9th state in the nation for identity theft victimization. In just two years alone, the crime of identity theft has risen 45% in this state alone, and I fear that Oregon will continue to experience increases in this crime because the state essentially lacks any meaningful legislation to help stop and minimize the effects of identity theft.

Identity theft is also a very real threat to commerce on the internet. A recent consumer study, conducted in just February of this year, by RPS, found that 25% of online shoppers, say they have reduced their buying over the internet in just the past year because of the threat of victimization. That portion is up from 6% two years ago who said they’ve cut back on their web shopping. I suspect these figures may be even greater right now since the poll was taken in February and since that time, we have all learned of the widespread security breaches of personal information occurring by industries across this nation.

To provide some context to our conversation, I’d briefly like to address what exactly I.D. theft is and how it occurs. I’m sure each of you have heard about the crime of I.D. theft, but just to make sure we all have a common point of reference, identity theft is when someone uses your personal, sensitive information without your permission, to commit fraud or other crimes. As I mentioned however, how the thief gains access to your personal information and how they use that information does vary widely.
As to how the thief uses your personal information, in terms of financial types of identity theft, there are two general categories. First is the use of an existing account, such as your credit card or your bank account. The second is the creation or opening of a new account in your name, such as taking out new credit cards, applying or receiving for loans in your name, or even receiving medical treatment under your name. When a thief opens a new account in your name, it is the most serious and costly form of identity theft. The federal trade commission estimates the average loss from the opening of one new account is more than $10,200, and the individual victim will spend more than $1,000 out of their own pocket trying to correct the problem. Again, how the thief gains access to your personal information occurs in many different ways.

When the crime of identity theft first started to gain national attention, most people thought of an identity thief as an individual who goes through your mail, goes through your trash, goes through your garbage, steals your purse or wallet, or even fishes possibly later on the internet. And indeed, as you can certainly become an identity theft victim in any one of these manners. As well, most of the public information that we tell consumers about how to protect themselves deals with this kind of method of taking your personal information. So, consumers are warned to get locking mailboxes, shred their trash which contains personal information, not to carry their social security numbers or give their social security numbers out over the internet or the phone. Consumers have been given the impression that if they changed their practices, they can protect themselves from this crime. They can protect themselves from becoming a victim of I.D. theft. Now, I absolutely advice consumers to protect themselves following these proceeding recommendations, however, it has become abundantly clear that consumers cannot, by their own actions prevent themselves from becoming victims of identity theft. We as consumers, require additional protection by legislation to protect our personal, sensitive information, which we currently have little or no control.

2005 has clearly become the year of wide spread security breaches, meaning large companies or institutions that maintain our personal information for legitimate purposes, have been allowing our personal information to be accessed by unauthorized persons. Loosing or misplacing our information or even selling our information to rings of identity thief. For instance, Bank of America lost a data tape/database, with over 1.2 million customers personal information this year. Time Warner lost or misplaced 600,000 individual employee records. Lexis Nexis, an online database and data broker, had a breach of computerized data effecting over 310,000 consumers. MasterCard, in the largest known breach this year in terms of shear numbers of individuals effected, breached the credit information of over 40 million customers. But one of the most interesting and illustrated breaches for the purpose of explaining the legislation I’m proposing the state of Oregon adopt is the Choice point Security breach. Where over 145,000 individuals personal information was sold to an international ring of identity thieves.

Today, I’ll be giving you introduction to four Mona laws, which have been developed with the aim of preventing identity theft and providing relief to those who have already been victims. These Mona laws have been developed by the state public interest research groups, in conjunction with consumers union as you all may know is the publisher of consumer reports based on the best
practices of states who have already enacted and perfected such laws. There are four essential components that should be enacted in Oregon to ensure that Oregonians are protected from identity theft, and these components in brief, are, first, a notification component. Second, the protection of social security numbers, the key to an individual’s financial identity. Third, the adequate destruction of personal records containing sensitive personal information. And four, the ability to utilize a security freeze. Which I’ll explain in more detail.

Throughout this discussion, I will try and tie these proposed legislative reforms to real stories regarding identity theft to provide some context to these concepts. Which leads me to the story of the Choice point breach. Choice Point is a data and information broker meaning Choice Point’s entire business model consists of selling our personal information. Choice point maintains files on millions of individuals. These files contain such information as our social security numbers, our address, our employment records, public records, drug testing records, and the list of information they maintain goes on and on. In September of 2004, Choice Point discovered suspicious activity by a purchaser of their information, particularly one small business customer. Choice Point soon realized it had sold more than 145,000 individuals personal information to a criminal ring of identity thieves. However, not until February of 2005, more than four months after discovering the security breach, does Choice Point actually begin notifying individuals who’s personal information, including their social security numbers has been sold. Quite frankly, a CSO magazine said about this, they basically asked to be legislated. Initially, the interesting thing is, Choice Point only began to notify 35,000 of the 145,000 individuals, all of those 35,000 people lived in the state of California. Now, you, not unlike many people, may be asking yourself, why only notify Californians? The answer to this leads me to the first of legislative reforms, I believe the state of Oregon needs to enact, a notification law.

California had the foresight to enact a law requiring both public and private entities to notify California residents when their personal information had been breached. At the time, California had the only notification law in place, and thus the residents of any other states didn’t initially receive notification. Only after the attorney generals of 38 states demanded that their state residents receive notification, did Choice Point actually begin notifying people from Oregon, Washington, and any other place besides California. Since the adoption of the California law, and in reaction to the numerous security breaches, as the Choice Point breach, and ones I’ve already mentioned, at least twenty-one other states now have notification laws, however, Oregon does not. Thus, Oregon residents have no guarantee that they will receive notification when their personal information has been breached by a third party. Besides actually having a notification law, the particulars of such a law are extremely important to insuring that consumers are adequately protected. A strong notification law is essential to preventing individuals from becoming victims of I.D. theft. The basics of such a strong law would be, immediate notification upon breach.

Some states under pressure from industry have enacted laws with what I entitled “too much wiggle room” or “the wiggle room laws”. It’s a cause that doesn’t adequately protect the residents of their state. What it does is, allow the company to do an investigation and determine the reasonable likelihood of harm. Now, you might be saying to yourself, “well that makes sense,
if it isn’t reasonably likely that there’s gonna be harm, why send the notice?” Well, one of the major problems with the flaws of this type, besides leaving consumers vulnerable, if an entity makes an incorrect determination, is time. Identity thieves are extremely savvy and very quick. They know that they only have a limited time to take advantage of having your personal information for their financial benefit. By the time and entity investigates or determines that something may be reasonably likely, days, weeks, even months have possibly gone by, time in which identity thieves have certainly taken advantage of. For instance, in the Choice Point incident, within a matter of a few short weeks, before anyone even received notification, more than 750 confirmed individuals were victims of identity theft because of that breach.

Another major component of a strong notification law is exactly who has to report when they have a breach. California statistics on notifications in their state show that one of the entities who breach information frequently are government entities themselves, and quite frankly, colleges and universities being the highest. Obviously, government entities, including colleges and universities, maintain a lot of personal information on citizens. A strong and protective notification law would require both public and private entities to notify consumers of a breach.

And the final component of a strong notification law, which I will discuss with you today, is what type of information it should apply to. A notification law should apply to computerized data, which is both encrypted and non-encrypted. As I’m sure your aware, even a sophisticated hacker can access even encrypted data. So, it’s essential that encrypted date be included as well. Also, although what I have been talking about has primarily involved computerized data, it’s essential that a notification law also cover non-computerized or old fashion paper data. When an entity discovers your personal information has been stolen, whether its computerized or non-computerized, consumers deserve to know. Consumers deserved the right to be able to protect themselves from becoming a victim.

Now, before I go into the second essential component of an identity theft prevention package, I’d like the backtrack to the Choice Point story for a moment. As I explained, Choice Point is a data broker, selling personal information on the open market. One of the pieces of information Choice Point sells is social security numbers. Now you may be saying to yourself, ‘well that doesn’t seem right, selling of social security numbers, that’s got to be illegal’. Quite frankly, it’s the same reaction I had when I first learned of data brokers, and it’s actually the reaction I had from a number of Oregon legislatures who I’ve talked to about this issue. However, unfortunately, I assure you, it’s legal and at least, well, there’s a minority of states that actually have protection for this. But it’s defiantly legal in Oregon. I’m sure your aware, that your entire financial identity is tied to your social security number to receive any kind of credit, loans, credit cards, you provide your social security number. So, protecting this number is essential to protecting people from identity theft. As I mentioned earlier, it’s one of the main things we council consumers to protect themselves, is their own social security number. So we also must ensure that entities that possess this information, which is the key to our financial identity, safeguard this information as well. So we need to stop the sale and trade of social security numbers.
In addition to stopping the sale and trade, to further safeguard our financial identities, we need to limit the use of social security numbers for unnecessary purposes. Many colleges and universities use social security numbers as identifiers, even going so far as to printing them on your ID’s, your student ID’s. That leaves you vulnerable to identity theft. I should have checked with Pacific University, I’m hoping you don’t do that. We also must ensure that social security numbers, when they’re not necessary, they shouldn’t be given out. For instance, on a standard job application, there’s no reason to have your social security at that point, it shouldn’t be given out, and you shouldn’t be required to give it out at that point.

Equally important, we need to limit companies from printing your social security numbers on items they mail to you. Many companies continue to print our social security numbers on mailings on asking us to apply for credit, refinance a house; this is completely unnecessary and puts each of us at greater risk for identity theft. Thus, a necessary component to any law would be adequately protection of our social security numbers.

Now, I’m gonna leave the Choice Point story for just a moment, and I’m gonna tell you about another incident, to explain another portion of the laws that we’re proposing, which occurred in the Portland Metro area, just after April 15th, tax time. To help illustrate the next component, which is the adequate destruction of personal records. A local tax accountant, which had been working on numerous clients’ taxes, decided shortly after tax time to get rid of the copies of her clients’ filings and associated papers. Unfortunately, for her clients, she placed these documents in a recycle bin on the street corner. She made no attempt to redact the personal information, nor did she shred the documents. I’m sure you can guess what happened. Dumpster diving thieves found her clients information, of course their social security numbers as they were on the tax filings there as, and her clients quickly became victims. Identity thieves do know their business, and they know exactly where they should look for information they need to commit their crime. They frequently dumpster dive in numerous business entities recycling and trash. Quite frankly, a good haul they can get from a lot of victims all at once, it’s a lot easier than going from residential dumpster to residential dumpster. As I mentioned earlier, we advise all consumers to shred and dispose of any documents containing their social security numbers or personal information. Obviously, so should a business entity. However, with the few exceptions for healthcare records, information obtained for credit reports, and employment records, there’s no general legal requirement that entitles you to protections that a business must actually dispose of your records properly.

Another example of failing to adequately dispose of financial personal records occurred just a few months ago at the former Best Western hotel in Beaverton. The hotel had been closed for a number of months, however the financial records of the hotel had been left abandoned in the building. The records included, employment applications, canceled checks, credit card receipts, and copies of driver’s licenses. Police first learned of these records when they found them on a person being charged with both methamphetamine possession and identity theft. Thousands of individual’s personal information, which had been stored in 29 full boxes, are know in possession of identity theft ring. There’s no way to get that information back, and there’s no telling how
many people possess that information at this point. These two situations precisely illustrate why the residents of Oregon deserve to know that their personal information that’s being maintained by legitimate entities, is adequately destroyed before it’s being disposed of.

About this point, you may be asking yourself, ‘well, with all these possible ways that my personal information can get in the hands of identity thieves, can we really ever help to solve this problem and put a dent in identity theft?’ And to that, I have two comments. Yes, we can stop and minimize identity theft. The state of California, whose adopted many of the pieces of legislation I have just mentioned, has been able to reduce the growth of identity theft in their state in the year 2004, well below the average growth of the other top 10 states, which is where both California and Oregon reside at the top 10 for ID theft victimization.

The other answer I have for you is that there is one measure, one consumer tool that we know can stop, does, can and does stop, the most costly and serious form of identity theft that I mentioned at the beginning of this talk. At the opening of new accounts in your name, and the tool is called a security freeze. While a thief’s use of your existing credit card can certainly be difficult and time consuming to deal with, no other form of identity theft is as devastating to the consumer, as costly, as time consuming, and possibly as life altering, is when a thief opens a new account in your name. As I mentioned earlier, the FTC estimates that, a thief will obscon with more than $10,000 when they open an account in your name. And you will spend more than $1,000 out of your own pocket to correct the problem. The average time spent to correcting a problem like this is over 600 hours of your own time. Just to clear up mess that the ID theft is made of your credit and quite frankly, your good name.

So, how does an identity thief go about opening a new account in your name? Well, to apply for new credit, a creditor looks to your credit report before extending any new credit in your name. This is precisely what happens when a thief applies for credit in your name. The thief, with a few key pieces of information about you, including your social security number, applies for instance, for a new credit card or a new loan. The creditor simply pulls your credit report and verifies that you are worthy of extending credit to. In essence, the credit report is able to be accessed by anyone at anytime with just a few key pieces of information. Without the ability to access your credit report, you may be powerless to stop identity thieves. However, if we give consumers the power to control access to their credit report, consumers can stop identity thieves in their track.

A security freeze is really just a fancy name for what essentially amounts to putting a personal identification number or a pin number on your credit report, not unlike a pin number on your ATM card. With this sort of essential control of our own credit report, consumers can have the piece of mind that they know, that they can prevent themselves from becoming a victim of new account identity theft. Simply, a security freeze is a tool that consumers initiate, or place on their credit by contacting the three major credit bureaus, Experian, Equifax, and Trans Union. When a consumer requests a freeze on their report, they receive a personal identification number. With the freeze in place, a consumers credit report and your credit score cannot be shared with any potential creditor unless you unlock access using your personal identification number.
As a result, even if a thief has stole your personal information an your social security number, their not going to be able to open fake new accounts or change vital information on your credit report, like your address, or your spelling of your name so they can easily access credit, take out new loans. The one thing that I will mention is a freeze does not at all hamper a consumers existing account, such as your credit cards. I think there’s been some confusion in some of the states that have looked at legislation of this type, that it will some how affect your existing accounts, and that’s really just not the case. In fact, all the states that have enacted freeze legislations specifically exempt relationships that you had with your existing creditors, that’s not the point of this legislation to hamper relationships with your existing creditors, it’s to prevent people from opening accounts that your not aware of. Thus, any creditor that you have at existing credit accounts can still access your credit report.

Ideally, a security freeze would be available to all Oregonians, at the present time, 12 states have enacted this type of legislation and the majority allows all their residents to use the freeze. A minority of the states have, a minority meaning 4 or the 12, have limited the use of the freeze to only victims of ID theft or those that have received notification that their personal information has been breached. While security freeze is defiantly an important tool for identity theft victims to prevent themselves from becoming further victimized, it is also an essential way of preventing identity theft from the outside. The ability of consumers to control access to their own credit report, their preventing themselves from becoming victims, is essential to stopping the identity theft epidemic and essentially restoring confidence in consumers, in their ability to use their credit accounts, in their ability to shop more on the internet, use eCommerce more fully.

So, in essence, I’d just like to briefly summarize some of the four main points I brought up in terms of legislation, that we believe should be enacted for real and substantial protections for Oregonians. The first is, a strong notification law applying to both computerized encrypted and non-encrypted data, as well as non-computerized data. A law requiring the protection of individual’s social security numbers including, the preventing of sale and trade of social security numbers by data brokers. A law requiring the adequate destruction of records containing personal information, and a law allowing Oregon consumers, the ability to control access to their own credit reports through the use of a pin number, otherwise known as a security freeze.

At this point, I would just like to thank you for your time. I would open up the floor to any questions you might have about identity theft legislation or any particulars.

Jeffrey Barlow

If I might begin, Shannon, and thank you very much. Those of us, like myself, who have had even a small problem with identity issues, are aware that, one, there are great many people out in society who have had similar problems. I was astounded when I went around to a few offices at Pacific University to make sure that I wasn’t having more complex problems as to how many of our staff have had such issues. So, we are at the point that this is indeed a very common crime and going up exponentially. So, I presume the time will come when it may even be the most common crime that many individuals are going to encounter within their lives. Where
should, given the lack of legislation in Oregon, the best thing I gather from what your saying that we can do, is to freeze that information to our credit accounts, to our databases.

Shannon Callahan
To freeze the information.....

Jeffrey Barlow
...for our credit bureau.

Shannon Callahan
It would be wonderful if we could; it’s not an option for us. It’s the option for resident

Jeffrey Barlow
We can’t do it at all.

Shannon Callahan
We can’t do it at all. I actually had a mother and daughter, or a mother call on behalf of her daughter. And she unfortunately had her information breached, in California, the daughter that was, and the residents of California were able to have all of their accounts, their credit reports, essentially frozen so that people couldn’t open new accounts in their name. But she wasn’t able to do that as an Oregon resident. At this point, Washington residents have the ability to do a freeze. Now theirs is limited to victims or those who receive notification. California is open to all individuals, and both of those states will go through receiving notification if there’s a breach of information, which I think really just leaves us here in Oregon, extremely vulnerable kind of like a big target for identity thieves. And there really isn’t anything that we can do to freeze our reports.

Now what I would recommend is that everyone checks their credit report at this point. You may have become a victim of identity theft and you don’t even know it, you probably wouldn’t know it until you would be denied for a new credit account and even then, only if you checked your credit report. We all are now entitled to one annual credit report for free from the three major companies. You can get that online if you so choose, you can also order it via the mail or over the phone and there is one central place that you can get that information at annualcreditreport.com. Do be careful, because there’s a lot of phony sites out there already, mimicking getting your free credit report and I would suggest that people check if they have concerns, they can get another credit report at a low cost.

I would not suggest identity theft monitoring services that they have, the credit report monitoring services. Those are extremely costly and quite frankly aren’t of very much help. But, you know, I think, I think one of the reasons I’m here today to talk is because I believe that each of us should start to advocate for ourselves, and without strong protections here in the state, we’re just sitting ducks. So, I’m hoping people will get more involved, start to look more at the issues, and be more active in advocating for yourself as a consumer and individual.
Jeffrey Barlow
Now, in fact, lacking that legislation however, even if we do monitor our credit checks, one would not detect thefts in process, but only accomplish thefts. So, there is going to be a lag, a month or even 6 weeks there that you would be vulnerable and not know it. So, even advising us to check monthly is not going to really solve this problem in the absence of decent legislation. It is terrifying. Questions?

Marc Marenco
One, sorry my voice is a little bit dodgy right now but I’ve been trying to sort out the, sort of the complex set of players and all of these kinds of activities that you’ve been describing. And I started writing a diagram; it’s gotten very complex. You’ve got the victim, you’ve got the thief, you’ve got the, you’ve got organizations that have relationships to the victim in which information is shared. You’ve got the credit recording groups that kind of siphon off information as a separate entity. And then you’ve also got new institutions that the thief may use to try and establish their place. And I’m wondering, this is kind of a fairly broad question for you but, thinking about, just about responsibility here for these kinds of spheres, um, and we talk about consumer rights and consumer advocacy and so on and so forth. I wonder how much of this at least as in part, a function of the fact that many of us consumers, we like convenience. And to be able to go online and to purchase the things quickly on Amazon is very timely for because, I was just about ready to buy a camera on e-bay, a video camera, an expensive one, and I got this offer to come back second chance offer, it looked just like the e-bay thing and so on, it had all the right graphics on it. So I started email corresponds with this person and about the third one through it said, well you know we can set up payments through Western Union. So, ok, you know, that might be right, and I said, “You don’t take Pay-Pal? Because in your ad it said you take Pay-Pal.” They said, “Well you know, I got burned last week on Pay-Pal so it’s kind of through Western Union.”

And make a long story short, is this close, well, I don’t know, I don’t know if I would have really put the money through Western Union. But I started corresponding with e-bay, it turns out bogus, and their now having me sort of play along, playing along to try and give e-bay time to find out maybe to get this person, this is a pretty substantial transaction over a couple thousand dollars. So, but you know, I, I was just a few clicks away from it and I gave all this information out, and I’m just wondering, you talking about consumer rights, you talked a little bit about consumer responsibility, but I’m just wondering if you can say a few things about this um, balancing this tension between security and convenience in a sense, that we all want this and how much, who’s gonna pay for the convenience, is this just the price of that?

Shannon Callahan
Um, I believe, that there are, as I mentioned earlier, that there are things we can do to really protect ourselves, you know, I’ve been getting those things about my Pay-Pal account, check here, and it says, oh you know, there’s a, it gives you all the language, like it’s a good little advertisement, you know, concerned about fraud, you know, it makes you think that it’s somehow legitimate and it isn’t. And some of that is consumers watching out for themselves, I mean there’s defiantly, you’ve got to look at, if it looks to good of a deal to be true, it is too good
of a deal to be true. And in terms of internet convenience, I think we can make the internet, in terms of general transactions, actually much more secure, I think a lot of the large companies have done that, I believe e-bay, Amazon, they have good standards, they have good ways for you to deal, obviously you should never send anything by Western Union, also never use your debit card, I think we all know that on the internet, your protection financially with using you debit card is not as great as with a credit card, you can dispute credit card charges, you have a lot more protection with a credit card than you do a debit card, quite frankly they can also take out all your cash out of your debit card and you could overdraft and there’s a lot of issues with that. So, I mean there’s a definite no-no on the Internet.

But you know, some of the things I’ve been trying to talk about today, one of the problems with identity theft is, if your dealing directly with the thief, you’ll know where you lost your information. Unfortunately, I think most people don’t know what happened when they become identity thieves, we just don’t know. And quite frankly, until this year, we’d never even heard of security breaches and to suddenly have breaches of peoples personal information that have approached 60, 70 million people, I think we’ve got to look at, maybe this has been going on a lot longer than we know. And I think that, you know, we need to do things at our own level, but we also need to look at what we can do to make sure that the information that we do use, um, and we do give out there is secure so that we don’t cripple this kind of Internet commerce activity. And quite frankly, I think we’re in jeopardy of doing that.

Unless, we put some actual, and there just common sense protections, we’re not talking about, really quite frankly, rocket science, it’s common sense things that I think most people, would think that they actually had some protection, I would think, that you would think that, a business would shred your personal documents and they would have some responsibility to do that, well they don’t, or, you know, I would think that business’s would notify me when they know that my credit card was stolen, well they don’t, and there’s no responsibility for them to do that. And unfortunately, think we may have to do a little bit of legislating and kind of rain this in, and we’re never going to get rid of identity theft, I mean lets just be quite frank, we’re never going to completely get rid of the problem. But how do we really minimize it, how do we do more protection, and how do we just do some of the common sense things that we can really do to stop it? And I think that’s why this package of legislation has been put together, and like I said, California grew at 11% last year, it’s still growing in terms of identity theft, but that’s, it’s the first state to ever see any decrease in identity theft numbers, and especially a state that has such a, has had such a problem with it in the past, they’ve normally been, quite frankly, number one. So, I think that we do see some things we can do, um, and again I would never say, I would never say a consumer should watch out for themselves, but unfortunately we’re not just dealing with what they can do.

**Jeffrey Barlow**

One of the things we’ve learned at the Berglund Center, is that in fact, many of these gangs are incredibly sophisticated, they are, they’re hackers if you will, are far better, more experienced, more trained, than the public servants who are charged with trying to deal with them. So, your
chances of successfully contending, via your personal computer, with these international gangs, some of which are out of the former Soviet Union, out of Holland, of course we’re all aware of Nigeria as well, are not good, lacking the kind of legislation that Shannon is, is speaking of.

Additional questions?

Marc Marenco
I still have more, but....

Jeffrey Barlow
In the back I think we have one, if you don’t mind, we’ll take....

Chad Wayne Potter
Chad Wayne Potter, I’m interested in the fact that we have some consumer laws on books now, we have an attorney generals office. How effective is the attorney generals office in handling this, or are they just simply wringing their hands?

Shannon Callahan
I believe our attorney generals office does what they can, but they, they are, the attorney general can only do what the law allows them to do, um, and quite frankly their budgetary constraints allow them to do. First and foremost is legislation, they do not have the ability with the current laws to actually require people to send Oregon residents notification. They can’t do anything about it. The attorney generals office was very active this year in trying to push the identity theft reform package, much of which, um, we’ve talked about today was actually contained in the bill in front of the Oregon legislature this year, um, a couple of different bills, and they failed to pass.

I believe that, you know, the attorney general will investigate fraud when they can, there’s so much of it out there though, it’s, you know, we would have to devote a full time agency to investigating all of it. I know that they look for patterns as much as possible when they get reports of these kinds of things; they look for the same patterns to go after, kind of the large fish as it were, to take those individuals down. But, um, they need some ability to go after people, and they really just, they can’t do anything about it, um, I mean they have some laws for criminal laws but, you know, there’s only so much we can do, and a lot of these criminals aren’t in Oregon. Um, you know, like Dr. Barlow mentioned, that identity theft ring from Choice Point was a Nigerian identity theft ring, you know, they’re doing a lot of funneling of money for, you know, the F.B.I. believes, quite frankly, terrorism. And so, there’s a lot of large international connections that we may not be able to control some of that, but we can control what happens to, um, to our own residence, and our own state.

Eva Crebs
I have a question. Um, you say that some of this legislation, Shannon, was put forward and it failed to pass. Why would legislatures not be in favor of protecting consumers?
Shannon Callahan

Uh, when we’re looking at consumer protection laws, there’s always a price to those who need to be regulated, um, it comes with a price for industry and different organizations, interesting enough, when we were discussing the protection of social security numbers, um, besides, uh, private industries that were concerned about the content, the government of the state of Oregon, was also very concerned about, um, some of these prohibitions as they would be required, or uh, thought they would be required to go back and have to redact social security numbers for instance, out of old family records filings, um, and some of it is trying to talk people through the legislation and what different things means, sometimes people don’t even know what a law means until a court interprets it of course. But, there’s been a lot of industry push, um, to be really frank with you on a lot of these issues the credit reporting agencies do not want people to have control over their credit report. They make too much money. They are selling crediting monitoring services now that are also a big source of revenue for them. Which we don’t really think is a value as doctor Barlow said you don’t really figure it out until after the fact, weeks, months after the fact. So there are some issues that are involved. Quite frankly there are not that many advocacies groups or individuals out there advocating for their own selves. And there are certainly a lot of industry representatives, i.e., lobbyists in the capital who have an ear, to some of the legislators. So unfortunately we just were not able to accomplish it and um, I believe that, I believe that we will be able to in 2007. Unfortunate, I believe the problem is just going to get greater.

Ted Krupicka

Hi, I am Ted Krupicka; I am with the ITC department here at Pacific. One of you solutions to security freeze seems to provide a solution for the major credit bearues, but I don’t see a solution for these data broker houses. Is there any type of solution to these people that are collecting data about you and how they resell that data?

Shannon Callahan

There, ah, some of the Choice Point has come out with some new guidelines for their own sale of information. I believe that we need to look at the large problem. Obviously, social security numbers are one particular issue. The sales of those are really our financial identity. If people saw what these data brokers were actually keeping on you I think you would be terribly frightened. I also think it is a big issue for people like victims of domestic violence or people who have stalkers, this information is readily sellable to a lot of different entities. I think we should probably look to severely limiting that to law enforcement and other purposes. Then again it is a huge business. This is how companies, you know companies, when they do a background search for high level employees or fraud will go and use these services to ensure that their employers are who they would want to hire. There are a lot of questions I think we all have to ask ourselves as a society which, is who should have access to this personal information and should we really start to limit these data brokers.

I, I believe at least in the case of social security number, I myself, believe I have the right to greater privacy. Personally, I think the information that they maintain is my information; this is my
personal option, not necessarily a commodity for buying and selling. But you know, I think this is a question we all have to ask ourselves and start to figure out, I don’t think people knew there were data brokers to this extent. I mean there are medical data brokers, there are lists and scores of people who maintain information that is truly, I think would, you know, not to kinda make people I am a black helicopter person. But once you start to look into this there are really some things that are of concern and I think we may want to limit the sell of this information.

Jeffrey Barlow
Thank you very much Shannon Callahan. I think the information that you are giving us is terribly important. The Berglund Center, our mission, is to study the impact of the internet on how we work and study and live our lives. And it is apparent that the internet is a mixed blessing in this regard, because the availability of these databases and this kind of information in the lack of decent legislation can be extremely threatening. And it threatens the internet itself. One of our concerns is simply that as this deluge of bad information continues to mound, fewer and fewer are going to be willing to trust the internet. Thank you for joining us today. Our next Berglund presentation will be on November 15th 2005 at Tuesday at noon. This speaker will be Reed Stager who is vice president for public policy at Digimarc Co. And Stager’s topic will be digital watermarking and public policy implication for both individual and corporate security. And he too will speak to the issue of private individual security as well as intellectual property rights. We hope that you will join us at that time. Thank You.

This entry was posted in Uncategorized by Editor. Bookmark the permalink [http://bcis.pacificu.edu/interface/?p=3204].

45 THOUGHTS ON “FEATURE: STATE LEGISLATION AND IDENTITY THEFT”

facebook stock
on January 30, 2014 at 11:53 AM said:

It’s actually a great and helpful piece of information. I’m glad that you just shared this useful info with us.

Please stay us informed like this. Thanks for sharing.

lose weight products
on January 30, 2014 at 1:33 PM said:

Wow, amazing weblog structure! How lengthy have you ever been running a blog for? you made blogging look easy. The overall look of your web site is great, as smartly as
Whitney Mcclinsey
on January 30, 2014 at 6:16 PM said:

Just desire to say your article is as amazing. The clarity in your put up is just nice and i can think you’re an expert in this subject. Fine together with your permission let me to snatch your RSS feed to keep updated with coming near near post. Thank you a million and please keep up the enjoyable work.

Jamie
on January 30, 2014 at 8:36 PM said:

It’s genuinely very complicated in this busy life to listen news on Television, therefore I just use internet for that reason, and get the newest information.

Nadine
on January 30, 2014 at 10:22 PM said:

Incredible story there. What occurred after? Good luck!

inbox blueprint review
on January 30, 2014 at 10:49 PM said:

It’s amazing in support of me to have a web page, which is useful in support of my know-how. thanks admin
Work from Home xbox support
on January 31, 2014 at 11:10 AM said:

Hi there, its fastidious post regarding media print, we all understand media is a wonderful source of facts.

---

best compact digital camera
on January 31, 2014 at 7:09 PM said:

Great web site you have got here.. It’s hard to find quality writing like yours these days. I seriously appreciate individuals like you! Take care!!

---

Jaclyn Edmond
on February 1, 2014 at 12:02 AM said:

Bonjour, Je voudrai apporter ma bijdrage à ce sujet si vous me Permettez. Merci.

---

Maxie
on February 1, 2014 at 5:23 AM said:

Hi there, just became aware of your blog through Google, and found that it’s really informative. I am going to watch out for brussels. I will be grateful if you continue this in future. A lot of people will be benefited from your writing. Cheers!

---

cash flow basics
on February 1, 2014 at 8:01 AM said:

For most recent information you have to pay a quick visit the web and on web I found this site as a best web page for most up-to-date
I love your blog.. very nice colors & theme. Did you create this website yourself or did you hire someone to do it for you? Plz respond as I’m looking to design my own blog and would like to find out where u got this from. kudos

It’s a shame you don’t have a donate button! I’d most certainly donate to this brilliant blog! I guess for now i’ll settle for bookmarking and adding your RSS feed to my Google account.

I look forward to fresh updates and will share this blog with my Facebook group. Talk soon!

Hello, Neat post. There is an issue with your web site in web explorer, would test this? IE still is the market chief and a big component to folks will pass over your magnificent writing because of this problem.
Hi I am so thrilled I found your blog page, I really found you by accident, while I was looking on Askjeeve for something else, Regardless I am here now and would just like to say cheers for a tremendous post and a all round exciting blog (I also love the theme/design), I don’t have time to look over it all at the moment but I have book-marked it and also included your RSS feeds, so when I have time I will be back to read a lot more, Please do keep up the superb work.

Lyle on February 2, 2014 at 2:10 AM said:

Hello there! I could have sworn I’ve visited your blog before but after looking at many of the articles I realized it’s new to me. Anyhow, I’m certainly pleased I came across it and I’ll be bookmarking it and checking back frequently!

circular saw reviews on February 2, 2014 at 10:36 AM said:

Hey there! Would you mind if I share your blog with my myspace group? There’s a lot of folks that I think would really appreciate your content. Please let me know. Cheers

Haraguchi Bovian on February 2, 2014 at 8:20 PM said:

Vivaldi 1 1/4ct TW Diamond Engagement Ring Set, in 14kt Gold $3,499.00

make money gaming
If some one wants expert view regarding running a blog after that i suggest him/her to pay a quick visit this web site, Keep up the good job.

Money Converter

Having read this I believed it was very enlightening. I appreciate you taking the time and effort to put this content together. I once again find myself spending a lot of time both reading and commenting.
But so what, it was still worthwhile!

social media addiction

Does your site have a contact page? I’m having problems locating it but, I’d like to send you an email.
I’ve got some ideas for your blog you might be interested in hearing.
Either way, great blog and I look forward to seeing it expand over time.

best folding bike

bookmarked!! , I like your site!

table saw reviews

If you want to take a good deal from this piece of writing then you have to apply these
methods to your won web site.

---

**best exercise bike**  
on **February 3, 2014 at 7:28 PM** said:

I was able to find good information from your blog posts.

---

**robotic pool cleaner reviews**  
on **February 3, 2014 at 7:46 PM** said:

Hi there, all the time i used to check web site posts here in the early hours in the break of day, because i enjoy to find out more and more.

---

**best garbage disposal**  
on **February 3, 2014 at 8:01 PM** said:

It’s a pity you don’t have a donate button! I’d without a doubt donate to this brilliant blog! I suppose for now i’ll settle for bookmarking and adding your RSS feed to my Google account. I look forward to brand new updates and will share this blog with my Facebook group. Chat soon!

---

**best vacuum for hardwood floors**  
on **February 3, 2014 at 9:11 PM** said:

What’s up, the whole thing is going sound here and ofcourse every one is sharing information, that’s really fine, keep up writing.
**best espresso machine**
on **February 3, 2014 at 9:18 PM** said:

When I originally left a comment I appear to have clicked the -Notify me when new comments are added- checkbox and now every time a comment is added I receive 4 emails with the exact same comment. Perhaps there is an easy method you are able to remove me from that service? Many thanks!

**make money growing weed**
on **February 3, 2014 at 9:29 PM** said:

I like what you guys tend to be up too. This type of clever work and exposure! Keep up the wonderful works guys I’ve included you guys to our blogroll.

**Starla**
on **February 3, 2014 at 9:56 PM** said:

Hi! I’ve been reading your weblog for a while now and finally got the courage to go ahead and give you a shout out from New Caney Texas! Just wanted to mention keep up the great job!

**infrared grill reviews**
on **February 3, 2014 at 10:37 PM** said:

I think this is one of the most significant information for me. And i’m glad reading your article. But wanna remark on few general things, The website style is wonderful, the articles is really great :D. Good job, cheers
**best electric kettle**

on **February 4, 2014 at 2:15 AM** said:

Excellent beat ! I wish to apprentice while you amend your web site, how could i subscribe for a blog web site? The account aided me a acceptable deal. I had been a little bit acquainted of this your broadcast provided bright clear concept

**success hasn't spoiled me yet**

on **February 4, 2014 at 2:31 AM** said:

I like the valuable info you provide in your articles. I will bookmark your blog and check again here frequently. I am quite sure I'll learn lots of new stuff right here! Good luck for the next!

**scroll saw reviews**

on **February 4, 2014 at 2:55 AM** said:

Hey there! This is kind of off topic but I need some guidance from an established blog. Is it tough to set up your own blog? I’m not very techincal but I can figure things out pretty quick. I’m thinking about creating my own but I’m not sure where to begin. Do you have any tips or suggestions?
Many thanks

**best home gym**

on **February 4, 2014 at 3:31 AM** said:

Sweet blog! I found it while searching on Yahoo News. Do you have any tips on how to get listed in Yahoo News? I’ve been trying for a while but I never seem to get there! Thanks
Hello there, I discovered your site by the use of Google at the same time as looking for a related subject, your web site got here up, it appears great. I have bookmarked it in my google bookmarks.

Hello there, simply was alert to your weblog thru Google, and found that it’s really informative. I’m going to watch out for brussels.

I will be grateful when you proceed this in future.

Lots of people will be benefited from your writing. Cheers!

Good day! This is my first visit to your blog! We are a team of volunteers and starting a new initiative in a community in the same niche. Your blog provided us valuable information to work on. You have done a outstanding job!

Whats up. Incredibly nice internet site!! Guy .. Beautiful .. Incredible .. I am going to bookmark your site and eat the feeds additionally...I am satisfied to uncover plenty of helpful info here inside the article. Thanks for sharing...

Lots of people will be benefited from your writing. Cheers!
These days the internet technologies supply us with a extremely certain possibility to pick what exactly one requires

nigeria entertainment news

on February 4, 2014 at 10:39 AM said:

Hmm it looks like your internet site ate my very first comment (it was really long) so I guess I’ll just sum it up what I had written and say, I’m thoroughly enjoying your blog. I as well am an aspiring blog writer but I’m still new to everything. Do you have any recommendations for novice blog writers? I’d absolutely appreciate it. [Woah! I’m incredibly loving the template/theme of this blog. It is simple, yet effective. Plenty of times it’s hard to obtain that “perfect balance” between user friendliness and visual appearance. I have to say you have done a superb career with this. Also, the blog loads quite fast for me on Safari. Outstanding Blog][Do you mind if I quote two your articles or blog posts as lengthy as I supply credit and sources back for ones site? My blog website is from the same area of interest as yours and my targeted visitors would genuinely benefit from plenty of the info you provide here. Please allow me know if this alright with you. Thank you][Hi would you mind letting me know which webhost you will be using? I’ve loaded your blog in 3 a variety of web browsers and I need to say this blog loads significantly faster then most. Can you recommend a great world-wide-web hosting provider at a trustworthy price? Thanks, I enjoy it][Fantastic website you’ve here but I was wanting to know in case you knew of any discussion boards that cover the same topics talked about here? I’d very love to become a part of community in which I can get guidance from other experienced people that share the same interest. In case you have any suggestions, please allow me know. Quite a few thanks][Hey! This can be my first comment the following so I just wanted to give a quick shout out and say I definitely appreciate reading your blog posts. Can you recommend any other blogs/websites/frameworks that go over the exact same topics? Enjoy it][Do you have a spam issue on this website; I also am a blogger, and I was curious about your situation; we have created some nice practices and we are looking to exchange techniques with other folks, please shoot me an email if interested.

businesses online

on February 4, 2014 at 1:35 PM said:

Hi there everyone, it’s my first go to see at this web site, and article is in fact fruitful for me, keep up posting these types of posts.
Hello my family member! I want to say that this post is awesome, great written and include approximately all important infos. I would like to peer more posts like this.

Ebooks are an excellent way to drive targeted traffic to your website. Potential customers appreciate the advice and information that is provided in ebooks. One of the other easy ways to make money fast, is creating your very own product.

I simply could not leave your web site prior to suggesting that I actually enjoyed the usual information a person supply in your visitors? Is going to be back often in order to check out new posts.

If you have a background in writing and have a good grasp in the English language, you can set up a website and offer your writing services there. These are discretionary items like a coke or a pack of gum, or eating out at restaurant. Getting the right crowd to see your website is a challenging task.