Justice Talking
Radio Transcript

Identity Theft: Protecting Your Good Name – Air Date: 2/27/2006

At least 7 million Americans are victims of identity theft each year. Criminals are stealing Social Security cards and driver's licenses, sending fake emails and "dumpster diving" to gain access to private information. It can happen to anyone and it can take years to repair your credit history after someone wreaks havoc on your credit. On this edition of Justice Talking we identify solutions for identity theft and ask whether Congress, state legislators and private businesses are doing enough to protect your good name.

MARGOT ADLER: From NPR, this is Justice Talking. I'm Margot Adler. Today we'll talk about identity theft, a crime that has hit 10 million Americans. You can become a victim without even knowing it, until you try to get a mortgage or buy a car and find out that someone has used your name to rack up thousands of dollars in stolen goods. As thieves use technology to expand the ways they can access your information, there are new ways you can protect yourself.

We'll also talk about what happens when colleges, hospitals or financial institutions accidentally leak your personal information, who is responsible and what can be done, and who ends up shouldering the cost of identity theft. Stay with us.

****

MARGOT ADLER: This is Justice Talking. I'm Margot Adler. We're talking about identity theft today, an issue that has affected millions of unsuspecting Americans. It has made a lot of us wary about how our private information is being disseminated. With each technological advance it seems that there are more opportunities for our personal data to be compromised. Later in the show we'll see what happens when a California man who has

been the victim of identity theft tries to get a department store credit card. And I'll talk with a privacy advocate and a representative from the financial services industry who disagree about what should happen when your data flows into the wrong hands. We'll also learn about "phishing" and how it relates to identify theft—and I'm not talking about using a rod and reel. We'll wrap up today's show with a conversation with criminal defense lawyer Alan Dershowitz, who shares his views on world politics and the use of preemption on the war on terror.

But first let's get a handle on just how big of a problem identity theft is in America. Joining me to give us some basics about identity theft and how many Americans are affected is Gail Hillebrand. She is a senior attorney at the West Coast Regional Office of Consumers Union, the nonprofit publisher of Consumer Reports. Welcome, Gail.

GAIL HILLEBRAND: Thank you.

MARGOT ADLER: What is identity theft?

GAIL HILLEBRAND: Identity theft is when someone pretends to be you in order to steal from someone else, to acquire goods or services.

MARGOT ADLER: Now tell me how identity theft typically occurs?

GAIL HILLEBRAND: It usually starts with stolen information of one kind or another. It could be as simple as your credit card number or it could be all your identifying information or it could be something important like your Social Security number. The thief turns the information into cash by running up bad debt in your name. They could do that by making charges on your current credit cards if they get that information; they can do it by taking money out of your bank account if they have your debit card number and guess your pin or steal your pin; and the most difficult form of identity theft to unravel is that they can do it by opening new accounts pretending to be you and running up a lot of bad debt.

MARGOT ADLER: We've heard a lot about information that's supposed to be kept under lock and key and gets exposed by accident by banks, hospitals, and universities. These are called data security breeches. How often does this lead to identity theft?

GAIL HILLEBRAND: It's very hard to know that, and the reason is that information can be stolen for use by thieves or it can be stolen for resale to thieves. So there's often a time delay between the time of the breech and the time of the misuse. But we do know that it's the area of your information that you can't control yourself. Someone else decides how much money to spend on protecting your information, whether it's worth it to screen and train their employees to encrypt the information they put on laptops that people might take out of the building and so forth.

MARGOT ADLER: How many people are affected each year by identity theft in America?

GAIL HILLEBRAND: In 2003 the Federal Trade Commission estimated 10 million Americans. There is a new industry-funded study this year saying it's 9.3 million. Either way that's too many people. And Consumers Union estimates that's about one American becoming a victim of identity theft every 19 minutes.

MARGOT ADLER: Wow. If your identity is stolen and your credit is damaged, what can you do about it?

GAIL HILLEBRAND: I always advise identity theft victims to start with excellent consumer materials at the Privacy Rights Clearinghouse site; that's privacyrights.org. They have a nice fact sheet that tells you all the steps you'll have to take—there are a lot of them. The Federal Trade Commission also offers advice. But generally speaking you are going to have to … well, it depends on what was stolen. If it's a credit card, only you can dispute those charges on existing accounts. If it's new account fraud you've got a number of steps ahead of you to notify both the creditors and the credit bureaus this wasn't me. And you always want to make those notices in writing, keep copies, and follow up to make sure that the bad debts are taken off your file.

MARGOT ADLER: You know, up until now I haven't really thought much about being super careful with personal information. I have to admit I throw credit card offers away in my trash, I put my credit card numbers on my checks when I make monthly payments and I don't shred anything. So what should I be doing?

GAIL HILLEBRAND: Don't recycle your junk mail. Tear up those credit card offers. You can also call and get on the Federal Trade Commission approved opt out list so that you get fewer credit card offers.

MARGOT ADLER: So I should be shredding everything.

GAIL HILLEBRAND: It's a good idea to shred anything that's got your card number on it or certainly your Social Security number. You can also try to get your Social Security out of your wallet. If your employer or your health insurer is using your Social Security number as an identifier number, ask them to change the practice.

MARGOT ADLER: So far what legislation is out there to protect consumers?

GAIL HILLEBRAND: There is one new tool that's kind of sweeping the states. We have it in 12 states now and 12 more state legislators are considering it. It's called the "security freeze." It doesn't stop your information from being stolen, but it stops crooks from turning your information into a new account in your name. And here's how it works. You tell the credit reporting agency, the big three credit bureaus, lock up my file, freeze access to my credit file. The information about your credit keeps going in and out of the file, so you know it doesn't stop information about whether or not you paid your debts from piling up, but it stops people who want to look at your account for purposes of authorizing new credit or new accounts, like a cell phone account, from looking at it. And then if you're the one who wants the new account, you unlock it with a password or with a pin.

MARGOT ADLER: So what gaps exist in current legislation? What do you think still needs to happen to protect consumers as far as legislation?

GAIL HILLEBRAND: We need laws in several areas. First, strong laws that require notice every time there's been a category breech. And the purpose of a notice law is to encourage companies to spend more money on security so that there are fewer breeches. It's not just to tell you, hey we didn't protect you. It's to encourage companies to protect us better. We need rules that require all kinds of companies that hold data to have internal security and protect that data. We need standards that allow us to see and correct information in these data broker files about us, and we need a right to place the security freeze without paying outrageous fees for it.

MARGOT ADLER: Gail, thanks for joining me today.

GAIL HILLEBRAND: You're very welcome.

MARGOT ADLER: Gail Hillebrand is a senior attorney in the West Coast Regional Office of Consumers Union, the nonprofit publisher of Consumer Reports.

****

MARGOT ADLER: You've probably heard many horror stories about identity theft. But the issue became personal for reporter Reese Erlich when his son Jason became a victim. And five years later Jason is still feeling the consequences. From San Francisco, Reese Erlich tells us the story.

REESE ERLICH: It was all my fault. I threw away an innocuous-looking change of address confirmation form sent to my son who was temporarily using my address. It turns out that's the first step identity thieves can use to redirect your mail and establish phony credit cards. Back in 2000 my son Jason Erlich was surprised to receive this letter from a major credit card company.

JASON ERLICH: "You've been approved for the Gold Option account. We're pleased to welcome you as a customer." So of course when I got this I was quite surprised that I'd have a $15,000 credit line that I didn't even know I wanted.

REESE ERLICH: At first he assumed there must be some mix up. Then three days later he got another letter indicating that he had taken out a large loan and then transferred the money to a stock brokerage account.

JASON ERLICH: Now this was a particularly shocking thing, because one, I hadn't opened up the account, and now they're saying that I had transferred it out. So it looked like whoever had opened up this account had transferred all of the money out of the account—$15,000.

REESE ERLICH: We contacted the credit card company to tell them he was a victim of identity theft. Luckily the company moved quickly and Jason didn't lose any money. When he applied for a real loan, however, his credit report still had the $15,000 phony charge. It took him many dozens of hours of making phone calls and writing letters to straighten everything out.

JASON ERLICH: It was pretty scary because at that point I didn't know what they had. Did they have just my Social Security number? Did they have mother's maiden name? Did they have my address?

REESE ERLICH: Many identity theft victims have suffered far more. But Jason wanted to make sure it never happened to him again. He filed a consumers alert with credit reporting agencies, which requires them to call him on his cell phone before approving any new credit applications. The alerts remain in affect for seven years—or so he thought.

JASON ERLICH: [getting out of a car] We're going to J.C. Penny to do a little shopping and see if my credit has been ruined or whether they're paying attention to fraud alerts.

REESE ERLICH: As soon as we walk into the J.C. Penny store a worker asks us to apply for an instant credit card which provides a 10 percent discount on any purchase. After buying some much-needed t-shirts and boxer shorts, Jason agrees to get instant credit. Jason provides his driver's license and Social Security number. Then in less than five minutes, Jason is approved.

STORE CLERK: You have $500 on your credit card, on your credit line.

REESE ERLICH: Okay. And that's it? Just instantly done?

STORE CLERK: Yes.

REESE ERLICH: No call to his cell phone, no mention of a fraud alert. But the error wasn't made by J.C. Penny or GE Consumer Finance, the credit card issuer. While Jason had filed consumer alerts with the three national credit agencies, one had removed it. And, as luck would have it, that's the one that GE checked. Critics say that even when fraud alerts exist, however, some retail stores, car dealerships and banks extend instant credit anyway, because they make more profits when people buy immediately.

Jay Foley, founder of the Identity Theft Resource Center says 38 percent of the victims his group surveyed had their fraud alerts ignored. Even if the account later turns out to be fishy, he says fraud amounts to less than one percent of sales for the $1.4 trillion industry.

JAY FOLEY: They're looking at that as minor inconvenience, where it's not inconvenient is to the individual who has to clean up the mess afterwards, the person who's had his own or her own credit dinged because of a fraud.

REESE ERLICH: Industry executives say that charge is unfair. GE Consumer Finance says it has fought hard to reduce identity theft, which has decreased markedly in recent years. Janine Movish is a senior manager of fraud and special investigations at GE Consumer Finance.

JANINE MOVISH: That was the fraud of choice for many perpetrators and that's why some of the prediction models that we've put into place, some of the data authentication tools that we've used, have brought that down by 70 percent over the last few years.

REESE ERLICH: She notes, however, that identity thieves are clever and constantly adapting to new anti-fraud methods. While fraudulent credit card applications may be down for now, that may not last.

JANINE MOVISH: I've been working on fraud cases for about the last 20 years and it's cyclical to be honest with you. We'll put tools in place and they might go a different route to commit the fraud and then they might come back and try that fraud again.

REESE ERLICH: So Jason and other identity theft victims must stay alert. One personal note: For the past five years I felt responsible for Jason's identity theft. It turns out it wasn't me. The change of address form was supposed to send Jason's mail to the identity thieves, but the post office screwed up and never diverted the mail, so Jason found out about the fraud right away. It took me five years and this story to find out. For Justice Talking, I'm Reese Erlich in San Francisco.

****

MARGOT ADLER: Just ahead we'll find out how your personal data may be accidentally leaked by your bank, your credit card company, your school or hospital. Don't go away.

****

MARGOT ADLER: This is Justice Talking. I'm Margot Adler. Once you are a victim of identity theft, life gets complicated when it comes to using and obtaining credit cards. What's the best way to protect yourself and whose responsibility is it? What should banks and credit card companies do to make sure their clients' information is protected?

To talk with us about all of these questions and more is Chris Hoofnagle, who is with the Electronic Privacy Information Center. He is a lawyer and privacy advocate there and directs EPIC's West Coast office. He joins us today from Chicago. Also joining us is Andy Barbour. He is vice president of insurance, technology and international affairs with the Financial Services Roundtable, a national organization that represents large financial companies. He is in Washington, D.C. Welcome Andy and Chris.

CHRIS HOOFNAGLE: Thank you.

ANDREW BARBOUR: Good day.

MARGOT ADLER: Let's talk about breeches in data security from credit card companies and banks. We've heard about data security breeches. That is when a client's personal information accidentally gets out. Chris you've said that the entire way that banks and credit card companies manage information makes security breeches bound to happen. Why?

CHRIS HOOFNAGLE: Security breeches occur because there's a very high reliance on the Social Security number in the financial services industry. So it's used often as an identifier, meaning how to figure out what your account is, versus someone else's. But it's also used as a password. So a single number cannot be used as both an identifier and a password. And a lot of the security breeches occur I think because of the reliance on the Social Security number.

MARGOT ADLER: Andy, shouldn't that be easy to change? Can't we just simply use other identifiers instead of the Social Security number?

ANDREW BARBOUR: Absolutely. And I think that that's happening. I mean, obviously Social Security numbers are a uniform identifier throughout the economy, including with the government, who uses it to process checks under their various mandatory payment programs. But yeah, financial institutions work with their customers to counsel them to do the things that they need to do to safeguard their accounts. We would never encourage anybody to use their Social Security number as a password to anything.

MARGOT ADLER: There is a fine balance between convenience and security when it comes to banking and finances. Shouldn't it be up to the bank, for instance, to make the judgment call on when to alert their customers to a security breech? What's the harm in that, Chris?

CHRIS HOOFNAGLE: I think that there is a problem there in that there's an incredible incentive not to give notice, not to bring negative PR to your company. And so generally the consumer protection advocates have argued that there should not be discretion. Now, I depart from a lot of the consumer protection advocates on this. I think that there should be some discretion amongst companies as to when to release security breech notices and when not to. However, the industry has responded to that by saying we only want to give notice where there is substantial risk of harm. And that's a very high threshold. I think if we look over the past couple years at all the security breeches we have seen, that standard would prevent consumers from learning about many security breeches that were in fact significant.

MARGOT ADLER: Andy Barbour, why shouldn't consumers be alerted each and every time a security breech happens?

ANDREW BARBOUR: Consumers should be alerted when they are at risk of identity theft, because we want them to take the steps that they need to take to avert the thieves from reaping any financial benefit in the first place, or if that's already happened unfortunately, from it getting any worse. You do run into a problem here though and this is the tension

that Chris is talking about, of having too many notices in the marketplace, of flooding consumers with notices that essentially direct them to do nothing and that don't mean anything. And what we don't want to happen is we don't want customers, our customers or consumers in general to become desensitized, especially in the instances where they really do need to take affirmative steps to help protect their identity or their finances.

MARGOT ADLER: Now one of the things that I've noticed—and I've had many charges, I have to admit, on my card that have not been mine—is that every single time the credit card company, American Express or Chase or whatever, has essentially paid the thing. Everything's been taken off, everything has been fine. And so my question to Chris is: Chris, if the credit card companies are standing behind me, standing behind all customers and take the hit, why does the consumer need to know if data was leaked?

CHRIS HOOFNAGLE: Well, it's a complex problem. It's a little bit nuanced here. On one hand when there is a fraudulent charge on your credit card, you don't have to pay the direct cost of that. But that cost is transferred onto you. It's transferred through higher fees, through interest rates. And ultimately onto the taxpayer because fraud is written off as a business expense. But the reason why you should know about security breeches is that if your Social Security number or driver's license number is acquired by another person, they can use it to commit more fraud against you.

MARGOT ADLER: Andy, are interest rates affected by this? Do taxpayers bear the burden?

ANDREW BARBOUR: I can't imagine that that is a substantial component of, you know, the general fee structure that financial firms charge their customers or the overall rate of credit or interest in this country. I mean, it certainly can't drive it any more than the cost of property or real estate or the investments that companies are making in technology, or what the central bankers decide. I wouldn't put too much stock in that, no.

MARGOT ADLER: But you represent hundreds of banks. You must have a clear answer to this.

ANDREW BARBOUR: No, I mean, it's sort of like, you know, what's the cost of a candy bar? I mean, if the price of sugar goes up by one cent per pound, is that being passed onto the people that buy candy? Well, if the price of aluminum or the foil that it's wrapped in goes down by two cents or has gone up by more, gone up by a nickel, I mean, how do you figure out what the component prices are? I don't have a definite answer. I acknowledge that to the extent that banks are losing a lot of money to fraudsters that they have to recover those costs somehow. But I wouldn't imagine that it's a significant component of interest rates or card rates.

MARGOT ADLER: Chris, have there been any lawsuits about security breeches?

CHRIS HOOFNAGLE: A number of lawsuits have been filed. Many of them are in California and the Pacific Northwest concerning companies that handle data poorly and thus cause some harm to other people. There's a case in California right now called *Harrington vs.*

ChoicePoint, which is a consumer class action against the company for releasing highly personal information to identity thieves, which was then used to commit identity theft. In that case the plaintiffs are alleging not only negligence but that ChoicePoint violated the Fair Credit Reporting Act. So I think we're going to see some lawsuits based on negligence for security breeches. And that should act as an additional deterrent, number one, for companies to stop collecting Social Security numbers. You know, it technically isn't a security breech if you don't have a Social Security number.

MARGOT ADLER: Now ChoicePoint was in another case where it settled for $15 million, right? So they must be in trouble, right? There have been several different situations.

CHRIS HOOFNAGLE: Well, ChoicePoint had a rather serious security breech where the records of 165,000 people were released to a ring of identity thieves. The reason why the case was so severe is that they didn't just get the Social Security number, they got entire dossiers and credit reports on these individuals. And then the identity thieves used those to commit financial fraud. And it appears as though they were looking for good customers. That is, they are looking for people with a lot of credit, and then stealing the identities of those people. ChoicePoint has settled with the Federal Trade Commission over the matter for a $15 million fine. But there are still private lawsuits.

MARGOT ADLER: I'd like to ask both of you what are the penalties that exist when companies have security breeches, and are they the right amount? Should they be higher? Andy, why don't I start with you?

ANDREW BARBOUR: Well, for financial firms we have to deal with our regulators, and ultimately the regulator has the ability to yank your license. And so the penalty is the ultimate penalty for a financial firm. If you got in too much trouble and acted egregiously and outside of the scope of regulation, you could lose your business over it.

MARGOT ADLER: Chris, what do you think the penalty should be?

CHRIS HOOFNAGLE: I've always thought this should be tied to executive compensation packages. You know, the Federal Trade Commission says that identity theft costs the economy $50 billion a year, and that cost is just being passed off onto consumers. That is, CEOs aren't taking a pay cut because of that level of fraud. And so I think that it would be a good idea to key those to executive compensation. Things might change.

MARGOT ADLER: Do you think that's outrageous, Andy?

ANDREW BARBOUR: I don't think that I'm in a position to agree with Chris on that one. [laughter]

MARGOT ADLER: Let's talk about credit freezes. I know, Chris, that you support them. Why?

CHRIS HOOFNAGLE: Because consumers don't have control over their credit report. Basically any retailer in America can pull your credit report today for very little reason. And once they've pulled your credit report they can issue credit. And so basically we think credit freeze is the solution because if people have control over their credit report and if they can control its dissemination, it will basically become impossible for identity thieves to masquerade as the victim and get credit in that person's name.

You know, we have examples of credit being issued to people who clearly were not the customer. They were clearly imposters. There are cases where people go to apply for credit and they have the right Social Security number but the wrong address, the wrong date of birth, and, in fact, they're in the wrong state. They don't even live in the same state as the victim. And stores are still extending credit.

There are examples of dogs getting credit cards, toddlers getting credit cards, young teenagers getting credit cards. There's a humorous story where a dog was issued a credit card after the owner received a pre-screened offer in the dog's name. The owner filled out the application by writing all zeroes for the Social Security number and wrote down that the dog worked at the Pupperoni Factory. And the dog still got the credit card.

MARGOT ADLER: Andy, what do you think are the downsides to credit freezes?

ANDREW BARBOUR: First of all, let me just say that I think that Chris makes a lot of good points and we would stand with EPIC side-by-side in working to find creative ways to reduce instances of fraud and identity theft. And one of the things that I think is in the marketplace right now, that I believe the Federal Trade Commission has already opined is working very well, are the amendments to the Fair Credit Reporting Act that were passed by Congress not but two years ago. And in those amendments there are additional consumer protections, red flag alerts, that you can put on your credit file, that you can request that the credit reporting agencies flag your file so that when there is a request for a credit report for the purposes of extending new credit, the requester has an affirmative obligation to contact the customer and verify they are who they are. Now, the ink is barely dry on those regulations, and the FTC has opined recently that they think the instances of identity theft are down. And I think that that has a lot to do with consumer awareness—people becoming more aware of the problems and people being more comfortable with what they need to do to lessen the chances of becoming a victim.

MARGOT ADLER: So Chris, what's the difference between these red flags and credit freezes?

CHRIS HOOFNAGLE: Most of the provisions in the amendments to the Fair Credit Reporting Act are remedial in that they protect you only after you're a victim of identity theft. So for instance, if you put a fraud alert on your credit report, you only put on that alert after you've become aware of fraud. Once you've put that alert on your credit file it only lasts for 90 days. So you have to continually renew that fraud alert. Not only that, that fraud alert is basically just an advisory note to creditors. Basically is says that they should be more careful when issuing credit to whomever shows up claiming to be the victim. What we've found in reality is that in about 20 percent of all identity theft cases retailers ignore

the fraud alert, and in fact there's nothing in the law saying that they even have to pay attention to it.

MARGOT ADLER: Andy, do you think that credit freezes are a reasonable option or do you think there are problems with them?

ANDREW BARBOUR: There's going to come a time obviously when this is debated on Capitol Hill, and I think that members are going to ask all the appropriate questions. One is obviously the mechanics of how credit freezes can work and at what expense. I mean, we have a credit-granting system in this country that is the envy of the world. It really is. And it was just reaffirmed by the Congress, like I said, in the FACT Act debate of a couple of years ago. And so at what cost? I mean, there are any number of speed bumps that you can put into the system. I agree that consumers need to have the highest level of protection. But there are always trade-offs, and as we talked about at the outset of this, there's a balance that you have to strike.

Now, I would say that I think that the red flag guidelines can stay on your account for up to seven years, not just 90 days. So there's a higher level of consumer protection there. But 13 states have legislated on credit freeze. It's not an overwhelming majority of the states, more may join. But I don't think there is a clear clarion call from customers out there to opt out of the credit-granting system.

MARGOT ADLER: There's been a lot of proposed legislation to deal with the issues that we've been talking about today. I'd like to ask each of you what you think the best proposals are that are out there. What don't you go first, Andy?

ANDREW BARBOUR: I think that what we're looking for here is some sort of uniform national standard, a strong national standard with appropriate consumer protections in it that says very clearly when and under what conditions customers should be notified in the event of data breeches. I think the other thing that there ought to be in the legislation is a national standard, national requirements for safeguarding customer information. As I mentioned earlier in this discussion, the financial services industry operates under a very rigorous regulatory system. But not everybody that has financial information or sensitive personal information lives under such regulation. So to the extent that all businesses, all entities, are required to safeguard information, I think that that would be an improvement.

MARGOT ADLER: Chris, what kind of legislation do you think we should have?

CHRIS HOOFNAGLE: There's no silver bullet to the identity theft problem. I really think we need to look at it from several different views. Andy is right in that financial services companies have been under a regime, a strong regime of regulation, for many years. And they get security better than a lot of other companies do. But there are a lot of companies out there that are using the Social Security number as a customer identifier when they don't really need to. So I think the first thing that needs to happen is to have less reliance on the Social Security number, both in the public sector and the private sector. I think

credit freeze is another great option. Finally, I do think that we should revisit the idea of negligent enablement of identity theft.

MARGOT ADLER: What is that?

CHRIS HOOFNAGLE: It's a bunch of confusing words, but it's basically the idea that you should be able to sue a creditor if they negligently grant credit to an imposter. So when you have a situation where someone who lives in a different state as you, who has a different date of birth, goes out and applies for credit and gets it in your name, shouldn't the retailer bear some responsibility for that error? Should you have to become a victim of identity theft and spend your time remedying the problem because a retailer was so sloppy in granting credit?

MARGOT ADLER: At this point I'm sorry we have to end our discussion here. I appreciate both of you coming on the show. Andy Barbour is vice president of insurance, technology and international affairs with the Financial Services Roundtable. And Chris Hoofnagle is a lawyer with the Electronic Privacy Information Center. Thank you both.

CHRIS HOOFNAGLE: Thank you.

ANDREW BARBOUR: Thank you very much.

****

MARGOT ADLER: Coming up we'll talk with Alan Dershowitz, one of America's most famous criminal defense lawyers, about how the United States could use preemption in world politics, what he thinks about Iran's nuclear power, the Israeli/Palestinian conflict and more. Stay with us.

****

MARGOT ADLER: This is Justice Talking. I'm Margot Adler. We've been talking about identity theft on today's show, about who is responsible for protecting your personal information and what you can do if you become a victim. But how do these thieves get access to our information in the first place? A lot of us have received familiar looking e-mails from companies we may or may not usually do business with. They've got the company logo and they seem legit, but oftentimes they're not. It's a practice called phishing and they are fishing for us to take the bait. Andrew Klein is an author and expert on phishing. Welcome, Andrew. What is phishing? Why is it spelled p-h-i-s-h-i-n-g?

ANDREW KLEIN: Well, the ph, I guess, came out of the late nineties, or something along those lines, where people were fishing for phone records, and the ph I think got used for that. It's been around that way for a long time. But phishing is an e-mail that arrives in your inbox that pretends to be from your bank or maybe e-Bay or an e-commerce vendor that isn't. And the idea of course is just to get you to click on a link, go to a website and

enter in some account information, identify information, financial information and so on—a very unscrupulous type of activity obviously.

MARGOT ADLER: Now, I should say that I do get phishing e-mails all the time that claim to be from e-Bay, from Pay-Pal, various banks. For people who haven't seen these e-mails, describe what they look like.

ANDREW KLEIN: Well, it looks just like it could come from your bank or from e-Bay or whatever, because it will have a logo usually on it, it will have the company information. It may even be sometimes addressed to you. Normally it says dear e-Bay account holder or dear Bank of America account holder or something like that. But sometimes they'll even put your e-mail address in there. So it will be dear you know aklein@abc.com or something along those lines. And it looks just like a regular piece of e-mail. That's part of what makes it difficult for people to detect. The better they are at convincing you that it's something that you should be expecting to receive, the harder it is to detect. And it always has a hook in there. Maybe that's why we call it phishing. It has to do something to get you to do an action. It has to create some type of a premise. So, for example, the recent transaction you posted on our website wasn't able to be processed because the credit card was invalid, please click here to revalidate your credit card. That's what a phishing e-mail looks like. And there are many different flavors.

MARGOT ADLER: Are people getting savvier about phishes?

ANDREW KLEIN: Oh, absolutely. We did a phishing IQ test about a year-and-a-half ago. And one of the things that we found when we first started doing it was that people weren't very aware of this. They missed almost half of the phishes. They couldn't identify them as a phish. They thought they were legitimate e-mail. And now what's happening is they're getting them right about 80 percent of the time. So people are becoming more aware. Now, the counter to that is the test also includes some legitimate e-mails and people are getting worse at finding legitimate e-mails. In other words, they're being…

MARGOT ADLER: In other words, we think that everything is a phish, so that we see the legitimate e-mail from our Chase Bank or whatever, and we say oh, my god, it must be a phish because, well, I'm worried.

ANDREW KLEIN: I think that's exactly correct. We err on the side of caution, which you know probably is a good idea.

MARGOT ADLER: Now who is doing all of this phishing? I mean, who are they and shouldn't it be reasonably easy to track them down?

ANDREW KLEIN: One would think, but what happened was that phishing started, let's say, three or four years ago, and it was done by mostly amateurs, but there's a fair amount of evidence now to indicate that there are organized teams of people doing this. And some people have even said organized crime. I don't personally have any indication of that but I suspect the government certainly does. But it certainly looks that way because you get to

see a lot of reuse of materials. Most of it is done offshore, outside of the United States, which makes it hard to track as you mentioned. It also makes it hard to process.

MARGOT ADLER: Thank you so much for coming on the show Andrew.

ANDREW KLEIN: You're welcome.

MARGOT ADLER: Andrew Klein is an author and expert on phishing tricks. He has created a test of your ability to detect a phishing e-mail. Take the test on our website, justicetalking.org. While there you can learn more about identity theft and how you can protect yourself from becoming a victim.

****

MARGOT ADLER: Alan Dershowitz is one of the most famous lawyers in the country. He has represented many famous people, including O.J. Simpson, Patty Hearst, Claus Vanbulo and Leona Helmsley. He's a law professor at Harvard University and has just written a new book called "Preemption: A Knife that Cuts Both Ways." Tell me what led to your consideration of the idea of preemption?

ALAN DERSHOWITZ: Well, actually I've been thinking about it for more than 40 years. I wrote my tenure piece in ancient history about the uses of civil commitment of sexual psychopaths and dangerously mentally ill people. So I've been writing about and thinking about prediction since the beginning of my legal career. But when 9/11 occurred and I heard the Justice Department official say we're now moving away from the business of only punishing crime we're moving toward preventing crime, preventing terrorism, and then the war in Iraq—preventive war designed to prevent the spread of weapons of mass destruction—it occurred to me that my original research now should be really relevant on the issue of a change in our attitudes. We're no longer deterring. We're moving much more toward a preventive mode.

MARGOT ADLER: Sort of like that movie "Minority Report."

ALAN DERSHOWITZ: Well, you know, I was actually a consultant to the studio on "Minority Report" because that's my expertise, trying to predict crime. But now it's minority report writ large—we're thinking about preempting or preventing the Iranians from developing a nuclear reactor, a preemptive strike in Iran, the way Israel conducted a preemptive strike against the Osirak nuclear reactor in 1981. Preemption is on everyone's mind.

One day last week I read a major newspaper and it had six stories on preemption in one day's newspaper, unrelated: New Yorkers passing a sexual psychopath law to preempt offenders, Israel targeted for killing the leader of the bomb-maker…

MARGOT ADLER: So how would you define preemption?

ALAN DERSHOWITZ: Well, preemption has to be distinguished from prevention. Preemption is when something's imminent. When a bomb-maker is about to blow himself up, you get him first, kill him before he kills you is what the Bible says. And that's preemption, if it's in immediate anticipation. Israel's 1967 attack on Syria and Egypt was preemption. On the other hand preventive war is very different. Well, in the long term maybe Iraq will be developing weapons of mass destruction, and we have to get them first.

Now preemption is much more justified than prevention in terms of warfare, but I'll give you an example of a preventive war that should have been fought that wasn't. Britain and France should have taken preventive action against the rise of Nazism in the 1930s when they violated their Versay Treaty. And the failure to do that, as Churchill has written and as Goering wrote, is what gave rise to the Nazi war machine.

MARGOT ADLER: You mention 9/11 as this sort of moment when there was such a shift and everybody talks about the world changes and so forth, but there's a part of me that wonders about that, that thinks you know, yes, it was this incredible tragedy and 3,000 people, more than 3,000 people, died, but what makes it so seminal?

ALAN DERSHOWITZ: Two things. What was unique about 9/11 were not the victims but the perpetrators. They were suicide killers. You can't deter suicide killers. You can't use the traditional threat of punishment to tell potential suicide bombers if you do this we'll kill you. If they're expecting 72 virgins in heaven, they're not going to be deterred. Now look, if we can persuade them that they're misreading their text, that all they get is one 72-year-old virgin in heaven, maybe we can desensitize them. But getting serious…

MARGOT ADLER: And you think that's really different? That the people who in Masada, the people who have laid down their lives for a cause, their whole life, that this is different?

ALAN DERSHOWITZ: Very different. This is very different. Historically people have risked their lives for a cause. But there is now a culture in some parts of the world of it's good to die, we have a culture of death. We welcome death. And I mean, one of the Iranian leaders said the other day about this cartoon that has been so provocative, he said Iranians are willing to give up their lives to protect the honor of the prophet—World War III staring over a cartoon. We live in a world now where the threat of punishment after the fact is simply not as effective. And that's I think why we've moved more toward a preemptive mode.

MARGOT ADLER: Now, you talk in your book about preemption, about wanting to create a jurisprudence of this notion. And I'm wondering if you could start the explanation of how we should think about when preemption is justified and when it isn't.

ALAN DERSHOWITZ: Well, that's the key. You can't say I'm against preemption or I'm for it. Sometimes it's going to be justified. It was justified in the 1930s against Nazi Germany. We will never know. By the way, had we done it in 1935 and destroyed the Nazi war machine, the world would remember a bunch of bullies—France and England beating up on a tin pan dictator who never would have gotten anywhere. We never would

have known about the Holocaust. If we do preempt Iran we'll never know whether or not they would have developed a nuclear bomb. And so one of the dangers of preemption and prevention is that you never know what you really prevented. And I think what we need is to begin to build a jurisprudence. We're doing it, but we don't have a calculus. We know better that ten guilty go free than one innocent be wrongly confined, after the fact. We have a calculus, but how many people should we overhear and surveil in order to prevent how many acts of terrorism? How many people should we preventively detain? How many people should we targeted kill the way the United States is now doing and the way Israel has been doing in order to prevent how many acts of terrorism? How certain do we have to be? What is the level of proof required? These are all the questions that go into building a jurisprudence and in my book preemption I try to build that jurisprudence based on our Constitution, based on our history and based on our values. But we're just beginning to build this jurisprudence.

MARGOT ADLER: Now when you take something that's been in the news lately, like let's say the NSA spying, how do you look at that from your own point of view?

ALAN DERSHOWITZ: Well, certainly you start by saying that some degree of preventive overhearing of planned terrorist attacks is justified. But should we allow the government without any authorization, without complying with the Fourth Amendment simply to monitor millions of conversations and then use a filter system to determine which ones to listen to? And Congress responds by saying well turn it over to FISA. FISA wasn't built for that, we didn't have this technology when the FISA law was passed. We need new hearings, new legislation, because this is a new form of prevention and preemption, this form of massive trolling and mining of data. And our prior model doesn't fit it all that well. That's why we need a new jurisprudence.

MARGOT ADLER: Now what does the U.S. Constitution have to say when you talk about preemption?

ALAN DERSHOWITZ: It doesn't say anything, because at the time the Constitution was written we didn't have wire tapping, we didn't really have preventive detention. Preventive wars had been fought, but there's nothing in the Constitution essentially about what the criteria for warfare is anyway. The Fourth Amendment talks about probable cause, but it contemplates an individual case, a specific target, whereas when we're trolling for conversations between Al Qaeda and people in America, you can't base it on probable cause, individualized probable cause. I don't want to rewrite the Constitution, because the Fourth Amendment has endured for so long, but it also says not unreasonable. And we have to ask ourselves what's not unreasonable, what is reasonable. In the context of new threats, new technologies, we have to control the technology and not allow it to control us.

MARGOT ADLER: When I hear you talk, I start thinking, well, it's very easy to have freedoms in peacetime. So are we in a situation where we only value the kinds of freedoms that we have in a time that's easy. And the minute we have, let's say World War II, well, let's lock up the Japanese.

ALAN DERSHOWITZ: Absolutely.

MARGOT ADLER: Is that the situation…

ALAN DERSHOWITZ: Five years, six years after we enacted the Bill of Rights we enacted the alien insidition laws because we were afraid of a possible invasion from France. Any time we've been at war the first casualty has been civil liberties, and then we react afterward and say oh my god, what did we do? We locked up a 110,000 Japanese. Let's past a statute. Or we had Watergate. Oh my god, let's pass the FISA law.

The difference is, of course, World War II ended on V-Day and VJ-Day, World War I ended. The war against terrorism will never end. It will always be a justification for increased powers on the part of the government to surveil, to prevent. That's why we need to begin the conversation about how to constrain the government, and we can't do it in absolute terms. We can't say no preemption or prevention, no targeted killings. If we got Osama bin Laden in our sites we would kill him if we couldn't arrest him. But we shouldn't be killing innocent people or people who are marginally involved. We need to know in a nuanced, collaborated way what is permissible and what's not, what's moral and what's not.

MARGOT ADLER: Now, you've I know made a lot of statements that were considered very controversial, saying that at times torture can be justified, at times preventive detention can be justified, etc. I'm wondering if you could talk about that.

ALAN DERSHOWITZ: Sure. I'm not an absolutist. I don't believe that laws come from mountain tops or from heaven or from prophets. I believe they are human contrivances, that rights come from wrongs. We look at experience and we create rights. There are no absolutes. I, myself, am opposed to torture. I would never want it see us use it. But we're using it. So what I want to do is see it regulated and controlled. I want to make sure it's not used the way it was used in Abu Ghraib. But if we ever had a ticking bomb terrorist who was planting a nuclear bomb in the city of New York, you think that anyone would hesitate to torture in order to get the information? Now, you don't believe anything obtained under torture. We would say to him, don't tell us where the bomb is, take us to the bomb. It would have to be self-proving. We would do it. And I want to make sure that if we ever do anything we have accountability, we don't have deniability. It's out in the open. There is democratic response and accountability. That's what's lacking today. Today we're torturing and we're hiding it—the worst of all possible worlds.

MARGOT ADLER: Thank you so much for talking with us, Alan.

ALAN DERSHOWITZ: Thank you very much.

MARGOT ADLER: Alan Dershowitz is a law professor at Harvard University. His latest book is called "Preemption: A Knife That Cuts Both Ways." To hear more of my interview with him, go to our website, justicetalking.org.