Radio Glencoe Podcast

It's the Law

Episode 4: Cyberlaw

ANNOUNCER
Welcome to Glencoe's *Business and Personal Law* podcast series. This is *It's the Law*.

SETH
Hello, and welcome to *It's the Law*. I'm Seth Abrams. Today we're discussing an area of the law that didn't even exist until recently, but that *everyone* needs to know about, and that is – *cyberlaw*. *Cyberlaw* is the term that applies to any laws related to computers. Joining us today is an expert on the subject, attorney Sara Kiefer, who will be taking your calls and e-mails. Sara, thank you for being here.

SARA
My pleasure.

SETH
As I mentioned in my intro, this is an area of the law that is still relatively new, correct?

SARA
Not only is it relatively new, but it is still evolving. As technology evolves, the law has to keep pace. And computer technology, as we all know, is evolving very quickly.

SETH
What's the most important thing our listeners should know about this area of the law?

SARA
Well I think we have to keep in mind that while the Internet has brought us many conveniences, from shopping online to instant messaging to paying bills online, you name it – it has also brought risks. And we are on the front lines as far as our responsibility to protect ourselves individually against *cypercrime*. *Cybercrime* is any criminal activity associated with a computer. As fast as the government can pass new laws against cybercrimes, criminals figure out new ways to commit them. So it's important for us all to know how to protect ourselves.

SETH
Just like we lock our doors to keep thieves from stealing our television, or not leaving our keys in the car, we have to be careful when using computers to do business.

SARA
Exactly. Sure it's against the law for people to steal from us, but they still do. Even when society gets up to speed in terms of fighting *cybercrime* with new laws – those crimes will still be committed. So we have to take precautions.

SETH
What's the most serious *cybercrime* threat out there today?

SARA
I wouldn't say it's the most serious, but it's the one every single one of us who uses a computer has to be conscious of, and that is identity theft. It's a huge problem, and fraud is on the rise too.

SETH
You mentioned that this is an area of the law that is still evolving. I'd like to read an e-mail from Roberto in San Jose who has a question along those lines. Roberto writes: "What is the government's approach to new technology, as far as keeping the laws current?"

SARA
That's a great question. It varies from state to state. Some states use the *cybertrespass* approach. That's where laws against crimes already in the traditional criminal code are used to cover the same types of crimes committed using a computer. For instance, if somebody steals your credit card from your wallet and uses it to run up charges at stores, that's already covered by the criminal code. If someone hacks into your computer to steal your credit card number and then uses it to charge things online, the same laws and punishments apply as if the person had stolen your credit card.

SETH
What are some other ways states are handling this problem?

SARA
Some states are writing all new statutes to cover every type of crime that can be committed using a computer. This is a lot more complicated, but some states prefer it because criminal law statutes have to be very specific. If a law is too vague, it can be difficult to prove a case, and the law could even be thrown out.

SETH
What are some types of crimes people commit using computers?

SARA
The criminal mind is, unfortunately, *very* creative.
As I mentioned before, identity theft is a very, *very* big problem. Identity thieves are obtaining personal data like social security numbers, birthdates, credit card numbers, passwords, PIN numbers, access codes, bank account numbers – the list goes on. They then use all of that information to run up credit card bills, or open new credit card accounts. They empty bank accounts, steal cash – it's terrible. And crimes like this can really damage a person's life, not to mention their credit. It can take years to recover from a crime like that. Other *cybercrimes* would include *cyberblackmail*, *cyberspiracy*, *cybervandalism*. Blackmail, conspiracy, and vandalism have all been around a long time, but now it's easier for criminals to commit those crimes using their computers.

SETH

Let's take a call from Samantha in Chicago. Samantha go ahead, you're on *It's the Law*.

SAMANTHA
I hear a lot lately about *cyberterrorism*. What is it exactly, and is it a realistic threat?

SARA
Cyberterrorism is when someone uses a computer to sabotage our national electronic infrastructure – things like the power grid, the air traffic control system, the national defense system, and the stock market. A *cyberterrorist* could disrupt transportation or communications, destroy records, or spread viruses that disrupt major computer networks. A lot has been done to prevent this from happening, especially since 9/11, but it's still a serious threat.

SETH
Well on that happy note, we need to take a quick break. Keep listening. We'll be right back.

ANNOUNCER
You're listening to Glencoe's *Business and Personal Law* podcast series.

SETH
We're back and we are talking with cyberlaw expert, Sara Kiefer. Sara, I want to talk a little more about *cybervandalism* – which you mentioned earlier. When does a computer prank become a crime? And what is the difference between a *cybercriminal* and a hacker?

SARA
Let me answer your last question first. There is no difference. A hacker is a criminal. Period. Lots of *cybervandals*, or hackers, may think what they're doing is just for fun, or an innocent prank. They might think it's a great way to get attention, or show off their brilliant computer. But it's still a crime. And let's not forget that there are hackers out there who have serious criminal intent and who are hacking into businesses or government computer systems purely out of revenge or as an act of sabotage. They are deliberately disrupting, damaging, or even destroying a Web site or computer network. These are very serious crimes, which come with very serious consequences. As well they should.

SETH
I have an e-mail from Lindy in San Diego who writes: "What can you do when somebody writes lies about you and posts them online?"

SARA
There's a term for that – *cyberdefamation*. That's using a computer to damage somebody's reputation, or a business's reputation, by deliberately posting false information online using e-mails or even text messaging. Congress recently passed an act called the Communications Decency Act that protects ISP's – Internet service providers – from being held liable for such acts. So that's a good start.

SETH
Is there such a thing as *cyberinvasion of privacy*?

SARA

As a matter of fact there is. It often occurs when people who – as part of their jobs – have access to our personal files. Confidential files like medical records, financial records, employment records – even school records. When these people use that information inappropriately, it's a crime. The federal government has passed several laws intended to protect us in that regard. And by the way, the two *cybercrimes* we've just talked about – *cyberdefamation* and *cyberinvasion of privacy* – are the two most common *cybertorts* today.

SETH
Glad you brought that up. Refresh our minds about what a tort is, and tell us the difference between a regular tort and a *cybertort.*

SARA
A tort is a private wrong committed by one person against another. So it stands to reason that a *cybertort*, is a wrong committed against another person using a computer – that is theft, falsification, misuse, or deletion of data stored in a computer to commit a tort.

SETH
I have a question, and I think a lot of people wonder about this. If you work for a company, are they entitled to monitor your e-mails?

SARA
As long as employers have your consent, and you are using company e-mail – yes they are. What many people don't realize is that they have agreed to that in most cases as part of their employment agreement or contract. I would say that a good rule of thumb is to never send an e-mail to anybody you wouldn't want your boss to read. It doesn't mean they will, but it's a good policy.

SETH
Okay we have time for one last e-mail, from Jason in Santa Fe, who writes: "What can we do to protect ourselves from computer viruses?"

SARA
From a legal standpoint, sending out viruses to destroy computer systems, or *cybergerm warfare,* falls into the category of *cybervandalism* or *cyberterrorism*. So sending out computer viruses is against the law, and those who do it are criminals. There are several ways you can protect yourself from computer viruses. Firewalls and anti-virus software, of course, can block many viruses. And it's a good policy to never open up email from someone you don't know.

SETH
I'm afraid we are out of time Sara .Thank you for joining us, and thank you for all of this terrific information.

SARA
My pleasure.

SETH
And as always, thank you for listening. Join us next time on *It's the Law.*

ANNOUNCER
You've been listening to Glencoe's *Business and Personal Law* podcast series.