As I have progressed through my career, privacy has always been a part of my job. However, for me, it is also a passion. It motivates me to write letters to congress people, pursue knowledge, and speak up in forums like this.

To answer the question, privacy is our friend, but the legal landscape and compliance is definitely our foe.

Today's session is not technical in nature. We will be exploring the roots of privacy and how we got to where we are at. We are also going to touch on a few of the privacy laws affecting our industry and finally close with a few things you can do to protect your own privacy and that of others. Hopefully, there will be nuggets you can take with you to help spread the word of privacy within your organizations and your personal lives.

To get started, what is privacy?

WHAT IS PRIVACY?

In the broadest sense, private information is any information about you that's nobody's business but your own, unless you decide to share it for a specific reason.

Privacy is the foundation for freedom of association, thought, and expression.

It is about an individual's ability to be free from interference, associate freely with whom they choose, and control the information that is available about them.

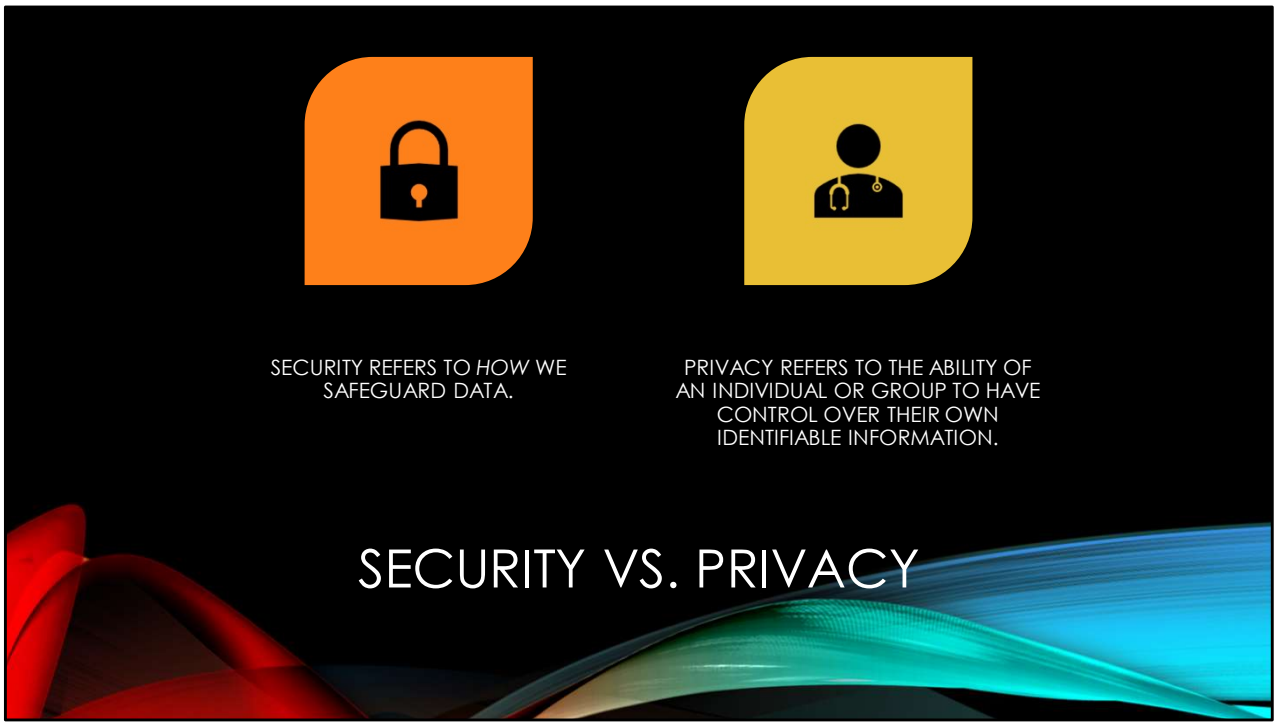
Physical privacy considers topics such as being frisked at an airport, providing a bodily sample for medical evaluation, or searching someone's personal belongings.

Information privacy refers to the personal information known about you, how it is used and disseminated in a digital environment.

In the broadest sense, private information is any information about you that's nobody's business but your own, unless you decide to share it for a specific reason.

Privacy is the ability to have control over how your personal information is collected and used.

Privacy is not security…



While security and privacy often appear together, they are not the same.

Security refers to *how* we safeguard data. It consists of physical controls such as passwords, locked file cabinets, masking information when it is displayed, etc.

Privacy refers to the ability of an individual or group to have control over their own identifiable information. Security is used to maintain privacy.

DIRECT DAMAGE

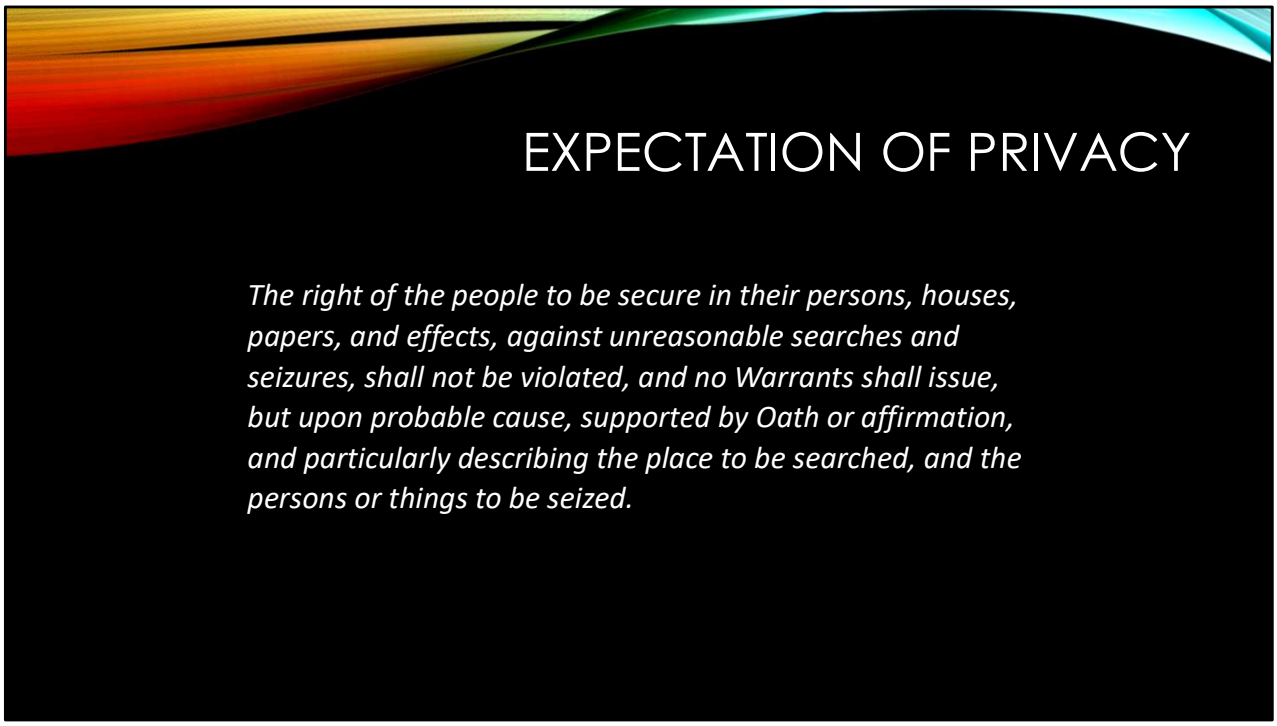
- Theft
- Social engineering
- Identity theft
- Stalking
- Fraud

And then there is the obvious. If the security side fails and someone has access to your secrets, they can use the information for a variety of evil purposes.

60% of Americans report they or an immediate family member were victims of fraud. Some examples of social engineering are simple, a phishing email or a phone call from Microsoft or the Social Security Administration. Many are more complicated with bad actors spending months developing relationships.

As of late July, the Federal Trade Commission logged over 500,000 reports of COVID related fraud resulting in 500 Million in losses.

But this is not a presentation on security, so let's take a look at the roots of privacy.



Over 150 country's constitution's have clauses regarding privacy. Our right to privacy is rooted in the 4th amendment.

First Amendment right to free assembly, and the Fourteenth Amendment due process right, have also been recognized by the Supreme Court as protecting a general right to privacy.

However, privacy is not directly addressed in any of our founding documents. The term privacy never appears.

To understand the basis for privacy in the legal setting, we need to turn to modern tort law.

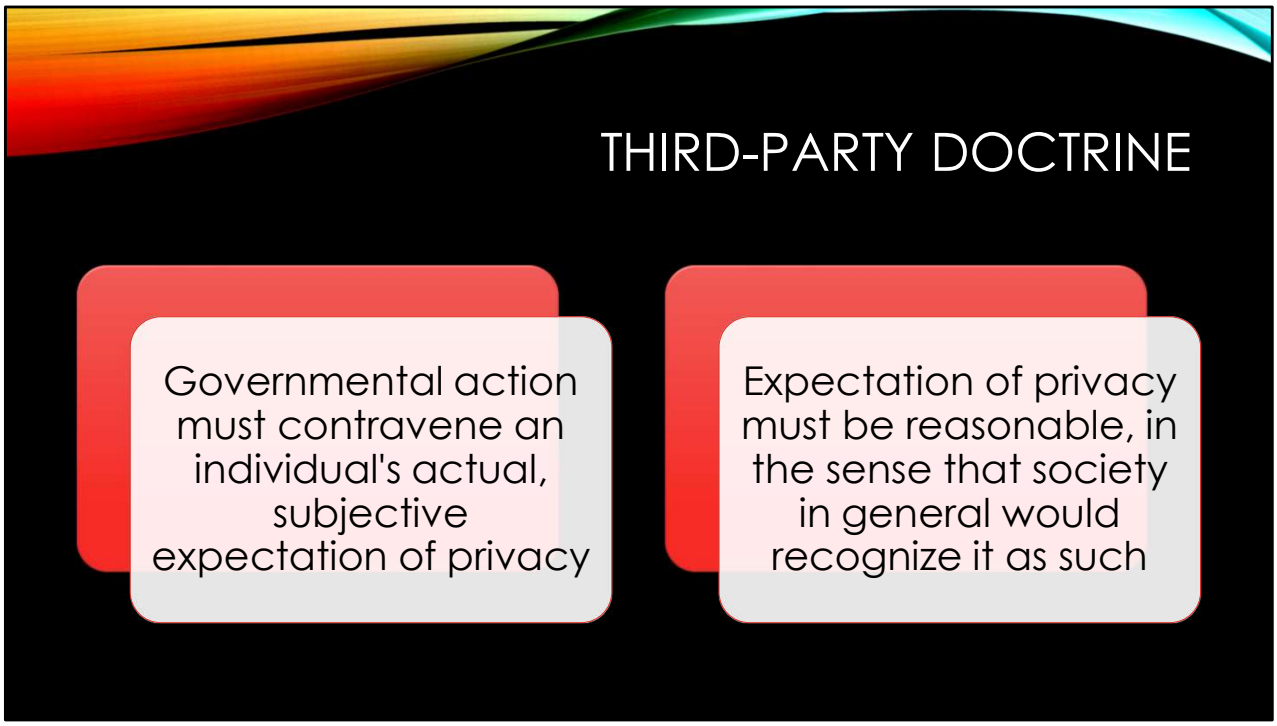
It is easiest to think of tort law as civil law. It is separate from criminal or contract law.

The purpose of tort law are to provide relief to injured parties for harms caused by others, to impose penalties on parties responsible for the harm, and to deter others from committing doing harm. Tort law is built on precedence rather than statute. It stretches back hundreds of years to first century Europe.

There are 4 categories in modern tort law related to invasion of privacy. Oh, and by the way, modern tort law began in 1870, so it is not too modern…

- Intrusion of solitude: physical or electronic intrusion into one's private space
- Public disclosure of private facts: the dissemination of truthful private information which a reasonable person would find objectionable
- False light: the publication of facts which place a person in a false light, even though the facts themselves may not be defamatory
- Appropriation: the unauthorized use of a person's name or likeness to obtain some benefits

Tort law has created a problem for privacy



Third-party doctrine has been the anchor of the privacy debate for decades. In Katz v. United States, (1967) Justice Harlan created a two-pronged test to determine if the 4th amendment applied.

The first test determined if the subject should expect privacy. This is centered around the concept of “in plain view”. Did the individual make efforts to conceal the information? For example, if a server finds a wallet left in a restaurant and opens it to look for contact information with the intent to contact the person who lost wallet,

finds illegal drugs, and calls the police, it would not be considered a violation of privacy.

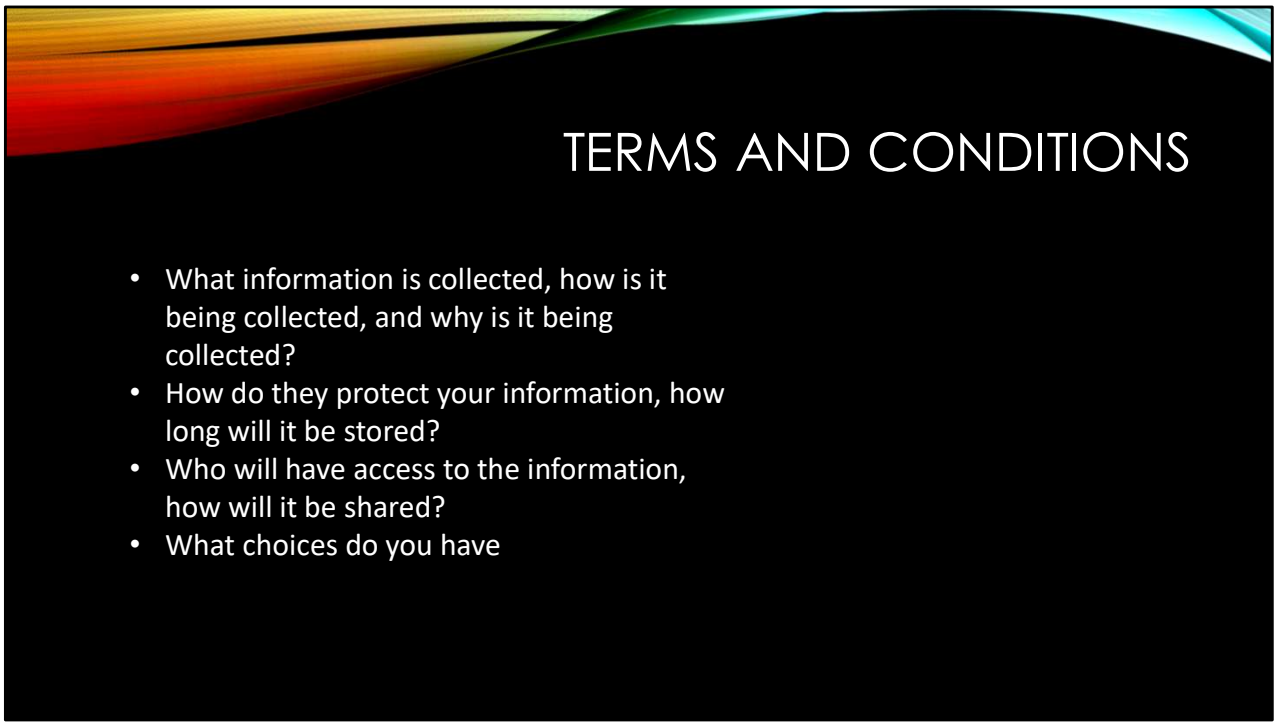
The second test is subjective. It asks whether a reasonable person would expect privacy in each situation. If someone threw their illegal drugs in the trash, law enforcement could search without a warrant as there is no expectation for garbage to be private.

This test created a problem for digital records.

In 1976 and again 1979, the Supreme Court affirmed that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties". This was found to be true even if the individual was required to provide the information to acquire the service.

In effect, this allow any third-party to share information you provided with other parties. This has created a problem for the digital age. Consider everything third-parties know about you - Every website you visit, every

search your make, all of your interactions with social media, everywhere your phone or car goes, everything you purchase on a credit card, the list goes on and on. In short, you have no right to privacy once you turn your information over to a third party.



Here are a few things to consider.

Because of the third-party doctrine, your information is only as secure as it is defined in the terms and conditions. This is why we carefully review the terms and conditions and privacy policy for all software and services in use at the institution.

In your personal life, I encourage you to review terms and conditions as well.

Raise hands if you think it was illegal. The official investigation recognized that no significant breaches took place, and no US criminal laws were broken. Furthermore, the investigation did not identify any data misuse by Cambridge Analytica and concluded that the methods employed were common and well-recognized and were based on widely available technology.

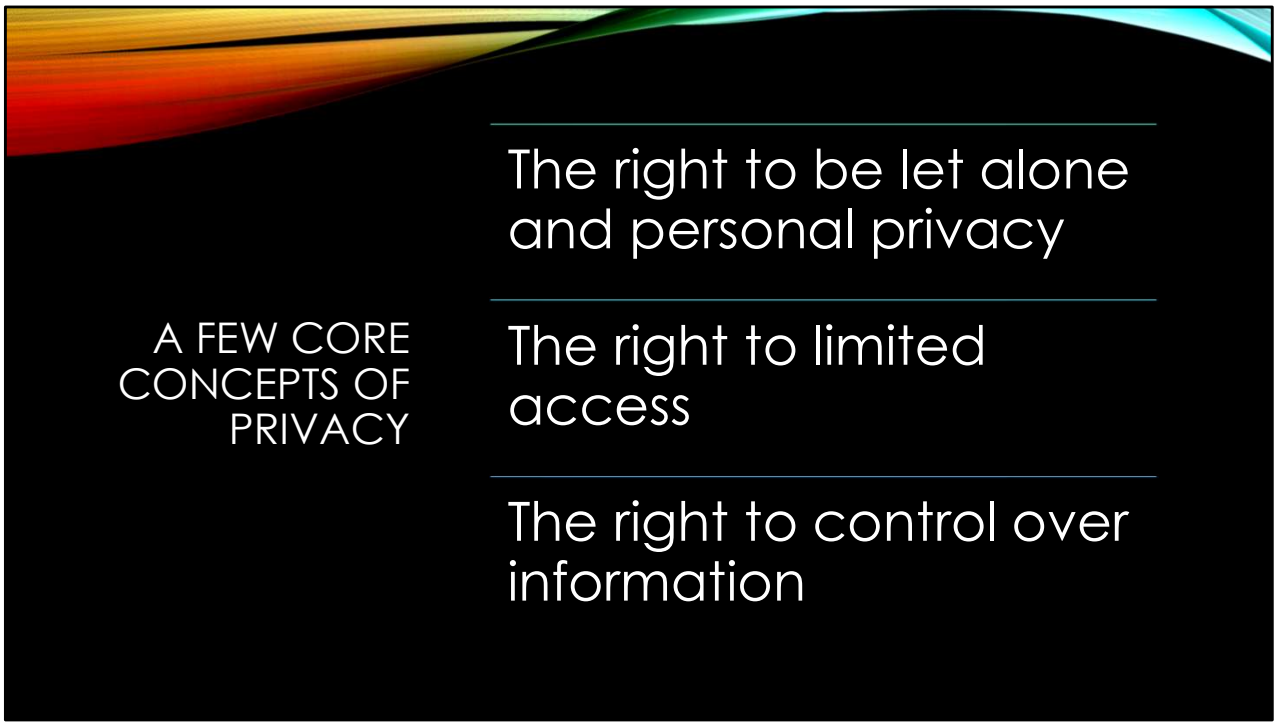
Although no criminal activity took place, Facebook broke their own terms and conditions. The Federal Trade Commission voted to approve a civil penalty of nearly $5 billion for breach of contract.

It would have been a violation of the European Union's General Data Protection Regulation and the California Consumer Privacy Act. However, neither law was in effect at the time of the incident.

People are beginning to respond to the third party problem. Our elected representatives are taking notice and proposing privacy laws across the country. Their efforts are beginning to be successful as we have seen with the California

Consumer Privacy Act, Illinois's Biometric Information Privacy Act, and GDPR.

Before we move on, let's take a look a few core principals of privacy and define a couple of terms.

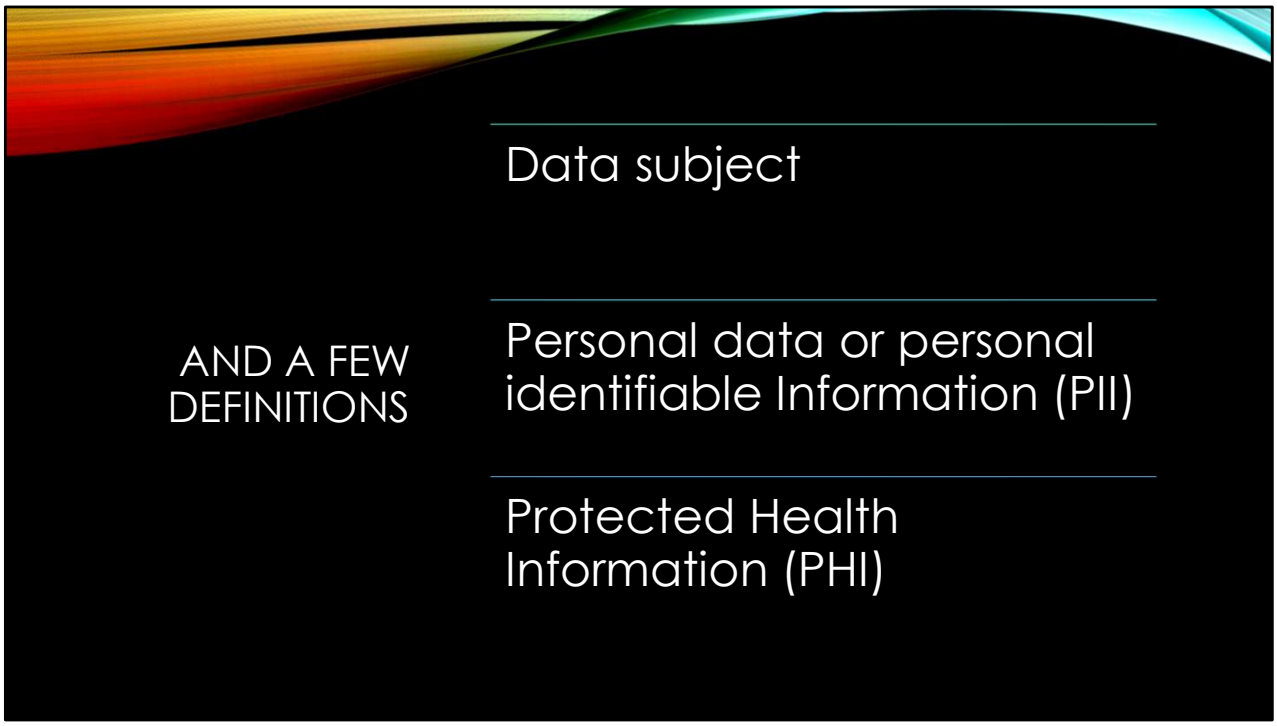


The right to be let alone and personal privacy. Your ability to seclude yourself from attention and prevent inclusion into your space. Your right to maintain private space whether it is within your own home or in a digital environment. It is the reason for doors on restroom stalls

The right to Limited access. Your ability to participate in events and activities without organizations collecting more information than they need to provide a service. Does the flashlight app you installed on your phone really need access to your contacts and location? Can you

control the membership in your social media friend group?

The right to Control over information. Your ability to control how information about you is shared with others. This is becoming more critical as we move deeper into a digital environment. It also anchors many privacy laws and policies.



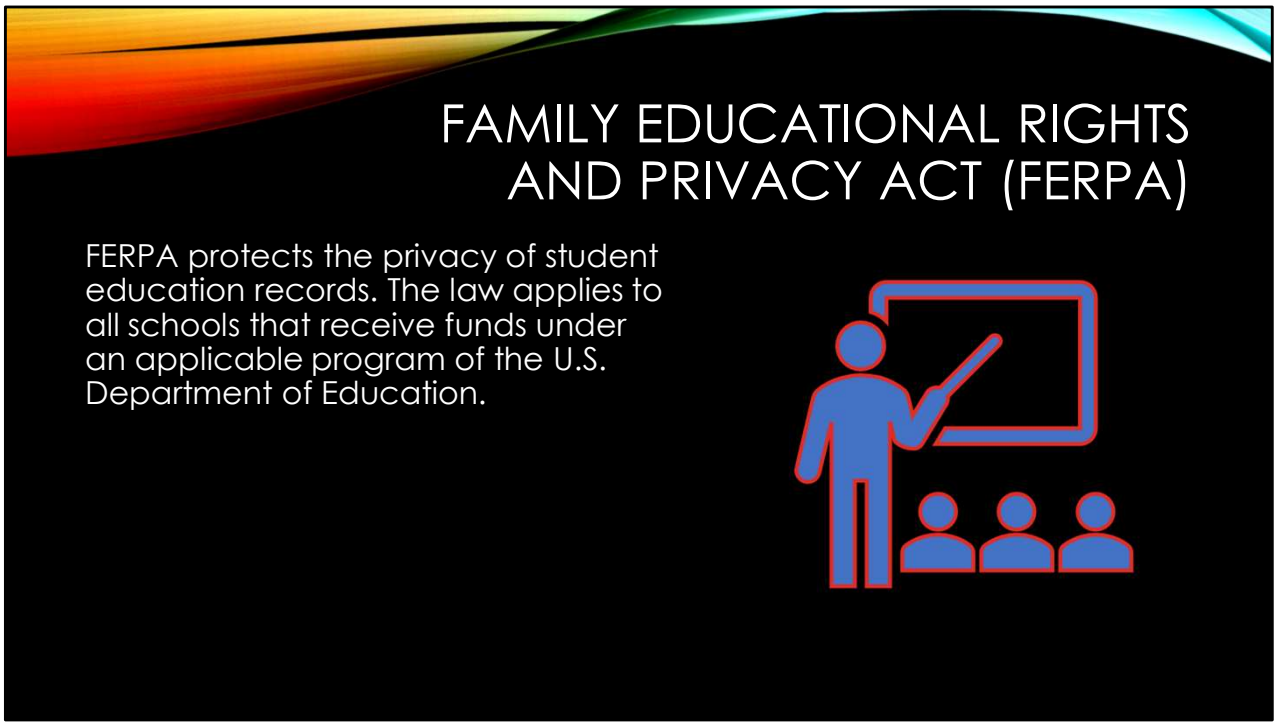
Data subject: An identified or identifiable natural person or group of persons to which Personal Data applies.

Personal data or Personal identifiable Information (PII): Information which can be used to distinguish or trace the identity of an individual alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual.

Protected Health Information (PHI): Any information about health status, provision of health care, or payment for health care that is created or collected by a HIPAA Covered Entity or a Business Associate of a Covered Entity

and can be linked to a specific individual (see HIPAA below). The term PHI is specific to HIPAA. For most purposes, PHI and PII are equivalent.

Now, off headfirst into privacy laws



FERPA protects the privacy of educational records. Nearly every record a college or university creates is protected by FERPA.

Interestingly, FERPA does not provide a private right of action. In other words, an individual cannot take action against a school for violating FERPA or sue a school for violating FERPA. They must register a complaint with the Dept of Education, who will then follow up.

Failure to comply with FERPA can put a universities' access to federal financial aid at risk. However, in its 47-year history, no college has ever lost funding due to FERPA. That said, the stick is big, so institutions do their best to comply.

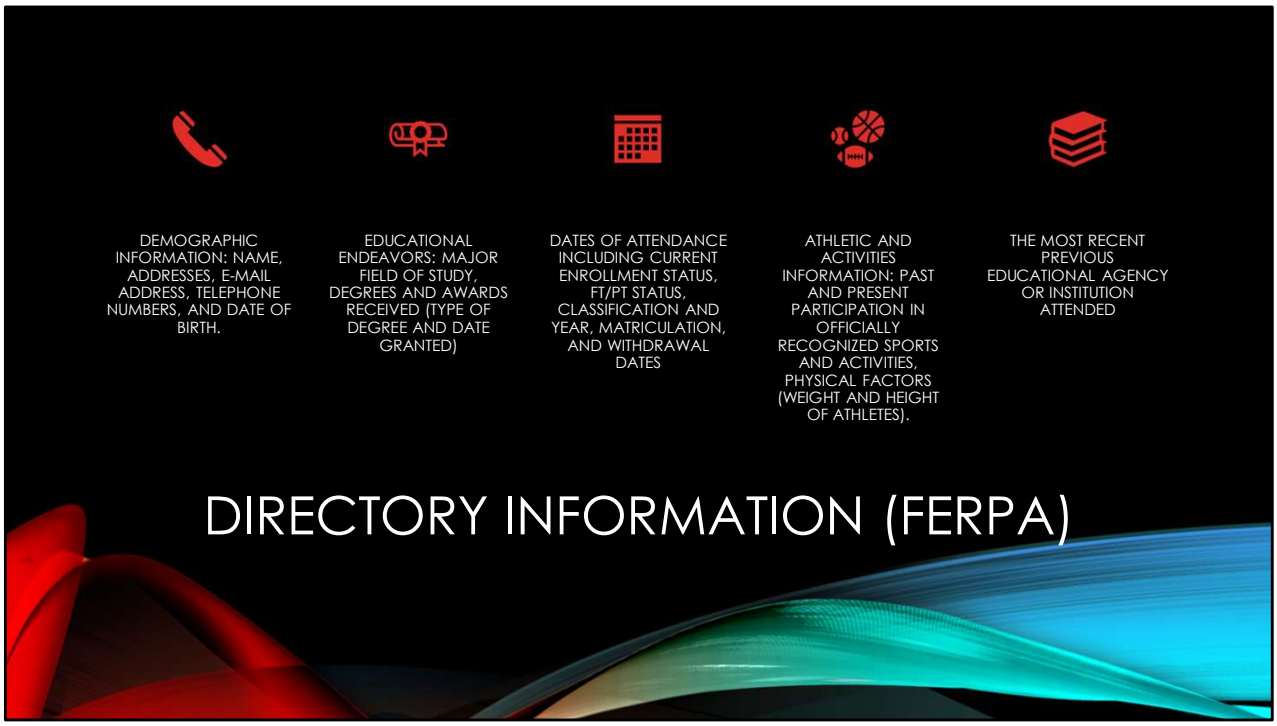
There are three core themes within FERPA…

REVIEWING AND CORRECTING RECORDS (FERPA)

Students have the right to inspect and review the student's education records maintained by the institution and students have the right to request that a school correct records which they believe to be inaccurate or misleading.

Institutions must provide students the ability to review and correct educational records. This can be very difficult in today's technical landscape. Educational records can be found across the institution and with the proliferation of services and providers, it can be difficult to keep track of what data the institution creates and where it lives. At my largest institution, we have classified over 500 systems and services that contain data. Of course, most don't contain educational records, but data asset inventories are classification efforts are key to compliance.

FERPA also allows institutions to share certain data

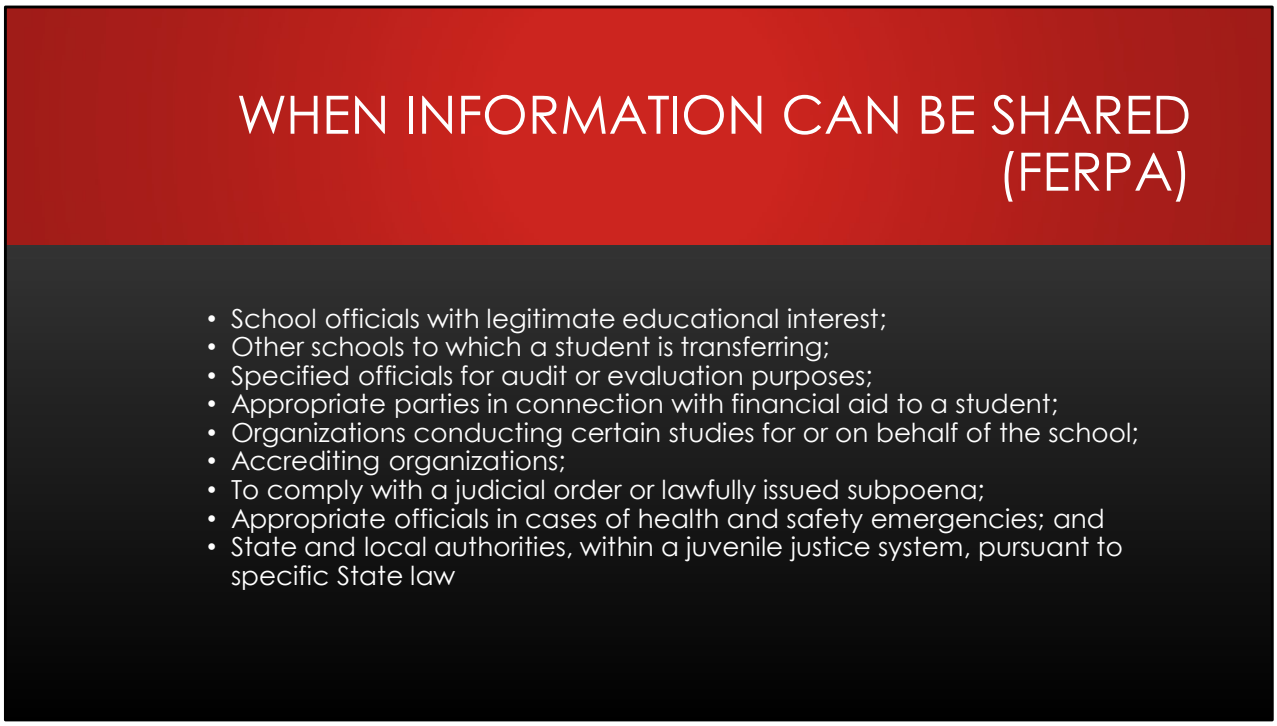


Schools must have written permission from the student in order to release any information from a student's education record. However, Schools may disclose "directory" information without consent. This is a list from one of my institutions.

Directory information is key to making systems work. It allows for address books, dean’s lists, and low-risk system integration. It is also important for data sharing with foundations and business partners.

However, it is important to remember, students have the option to opt out of allowing their information to be included as directory information. It is important that educators never assume they can share information just because it is included as directory information.

Finally,…



FERPA defines when an institution can share private data.

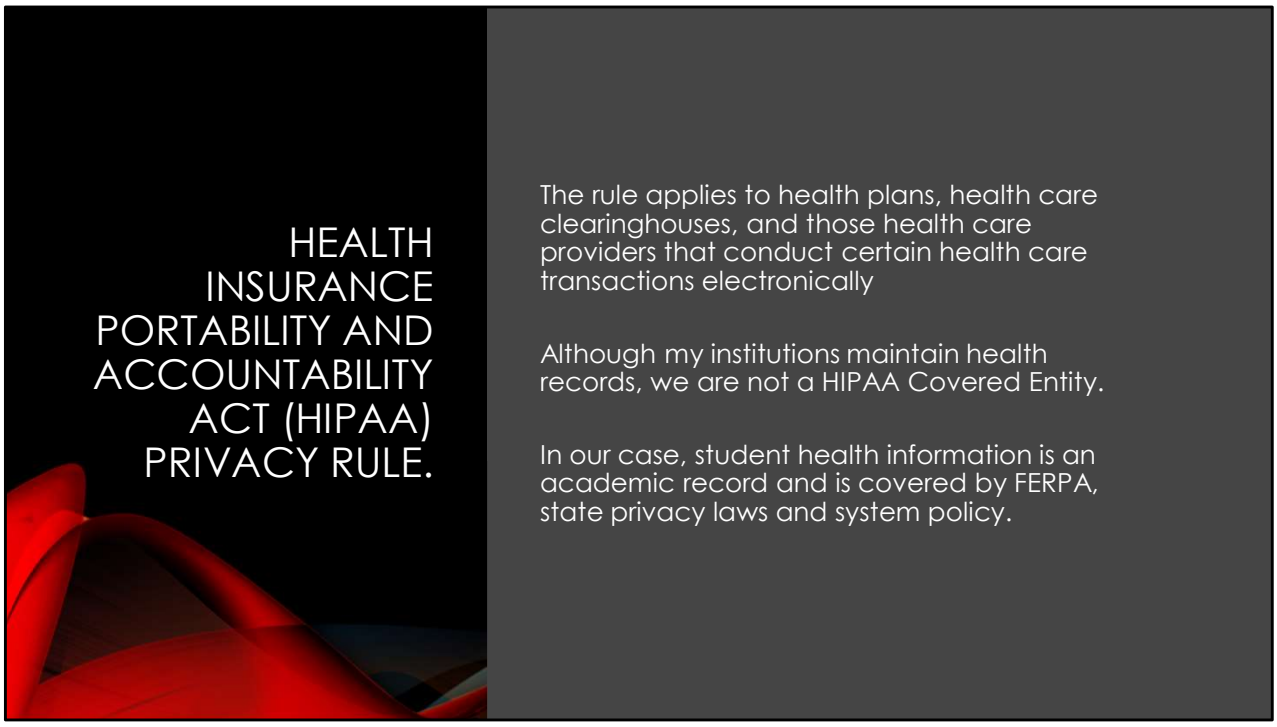
Most are self-explanatory. However, the first needs an explanation. In this case, “school official” refers to both employees as well as third-parties that has been contracted to provide an institutional service or function that would otherwise use their employees or systems.

The contractor must be working under the “direct control” of the organization in respect to the use and maintenance of educational records. In other words, the institution must maintain control over how the data is

used. This provision allows colleges to outsource services such as Microsoft Office365, hosted Learning Management Systems, and others.

It is important to remember, universities cannot store or process educational records in any cloud application or service without the appropriate contract language in place.

Now, let's take a quick look at HIPAA



This is a set of national standards protecting individuals' medical records and other personal health information. The Rule requires appropriate safeguards to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The rule also contains auditing requirements.

Like FERPA, the Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request

corrections.

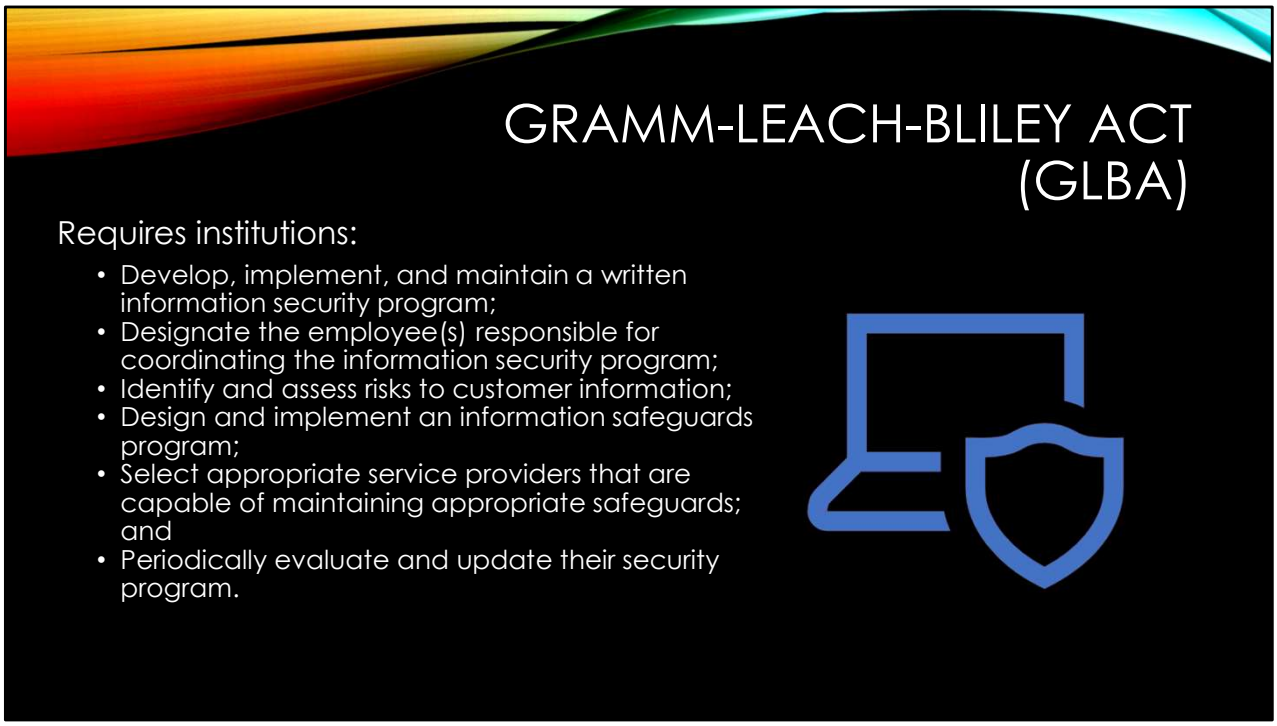
Violations result in fines from $100 to $50,000 per violation. Unlike FERPA, multi-million-dollar fines have been issued for flagrant violators. Some violations can also result in jail time of up to 10 years for the offender themselves.

The rule narrowly applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions where the department of health and human services has adopted a standard. These covered transactions are generally related to billing for defined services. Organizations that must comply with HIPAA are referred to an “Covered Entities”.

Although many colleges and universities maintain health records, they are not necessarily HIPAA Covered entities. HIPAA compliance can be costly. Institutions often outsource functions that would create a HIPAA compliance requirement such student health services billing, and more recently COVID testing providers who bill insurance companies.

From a public perspective, it is not too important whether something is FERPA or HIPAA. Both are high-risk, personally identifiable information and the organization is responsible for protecting it to a similar standard.

I could spend a whole session on FERPA, but it is time to move on to Gramm-Leach-Bliley



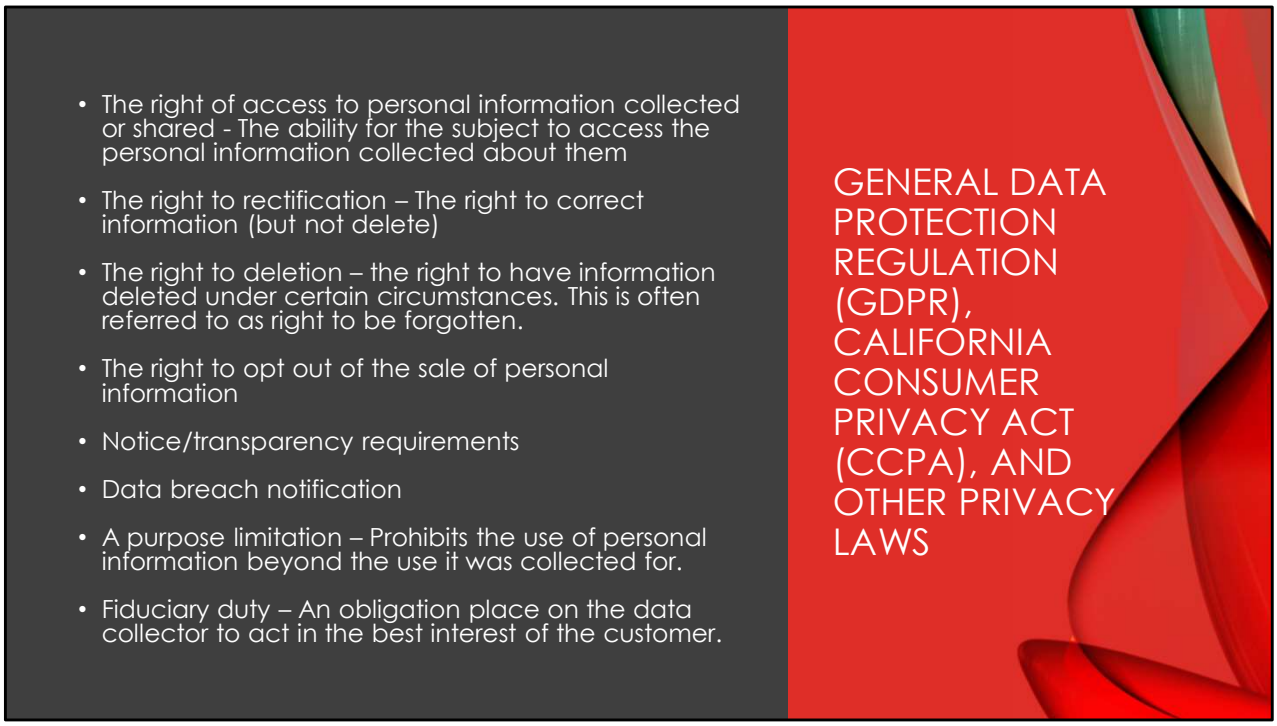
The Gramm-Leach-Bliley Act requires financial to explain their information-sharing practices to their customers and to safeguard sensitive data. Colleges and universities must comply with GLBA through their financial aid Program Participation Agreement with the Department of Education. Institutions are subject to federal audit under this agreement.

While FERPA and HIPAA maintain a focus on the data subject, GLBA focuses on building a robust information security program and implementing technical controls to

ensure the security of financial aid records.

- Financial institutions found in violation face fines of $100,000 for each violation.
- Individuals in charge found in violation face fines of $10,000 for each violation.
- Individuals found in violation can be put in prison for up to 5 years.

A bit of good news for me, the fines do not apply to colleges and universities. While they agree to comply, the Department of Education maintains procedures for enforcing Gramm-Leach-Bliley requirements. So, much like FERPA, the stick is the potential loss of access to federal financial aid.



The momentum to implement privacy law and policy is at an all time high. Currently California, Colorado, and Virginia, along with several foreign governments, have implemented privacy legislation. Most US states have privacy regulations working through the legislative process. Wisconsin's effort was killed in committee in April, but it is sure to be back.

Here are a few provisions that appear throughout the various regulations.

The variety of privacy laws has led to confusion. It is often difficult to discern what privacy laws may apply and what are the obligations of the data holder. Because colleges serve students nationally and internationally, this can be complex. Where the data subject is located, where the data is located, where the transaction takes place, all factor into the required response.

While not specific to privacy law, notification requirements are a good example. In Wisconsin notification is required within 45 days if over 1000 records were breached, credit reporting agencies must also be notified. Across the river in Minnesota, notification must be made “in the most expedient time possible and without unreasonable delay”. Credit reporting agencies must be notified if more than 500 records were breached. Colorado is within 30 days and 1000 records.

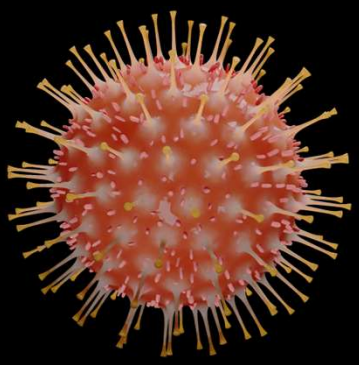
In the world of distance education, this can make any data breach response complicated. Thankfully, in my case, we rely on the UW-System Office of General Counsel in matters regarding privacy laws.

From a general user perspective, the takeaway is to understand that it is a complex topic, and a breach of privacy can be time consuming and costly. There has been talk of a federal privacy law but no action. This could be a tremendous benefit for companies struggling to comply with the current patchwork of privacy laws. I am not holding my breath.

So, let’s move on to your role in privacy.

That's really all there is too it. We all handle personal information in our jobs and in our personal life. You job is to protect it. However, there are a few principals to follow and things to know.

QUESTION FOR CONSIDERATION



You receive an email from one of your staff. They inform you that they will be absent due to a positive COVID diagnosis and provide a detailed update on their work progress and outstanding deliverables. You assign the workload to another employee within the department and forward the email containing the work progress and outstanding deliverables for them to address.

Is this a privacy issue?

Absolutely!

This issue recently happened to me.

A breach can be as simple as forwarding an email without stripping unnecessary private information.

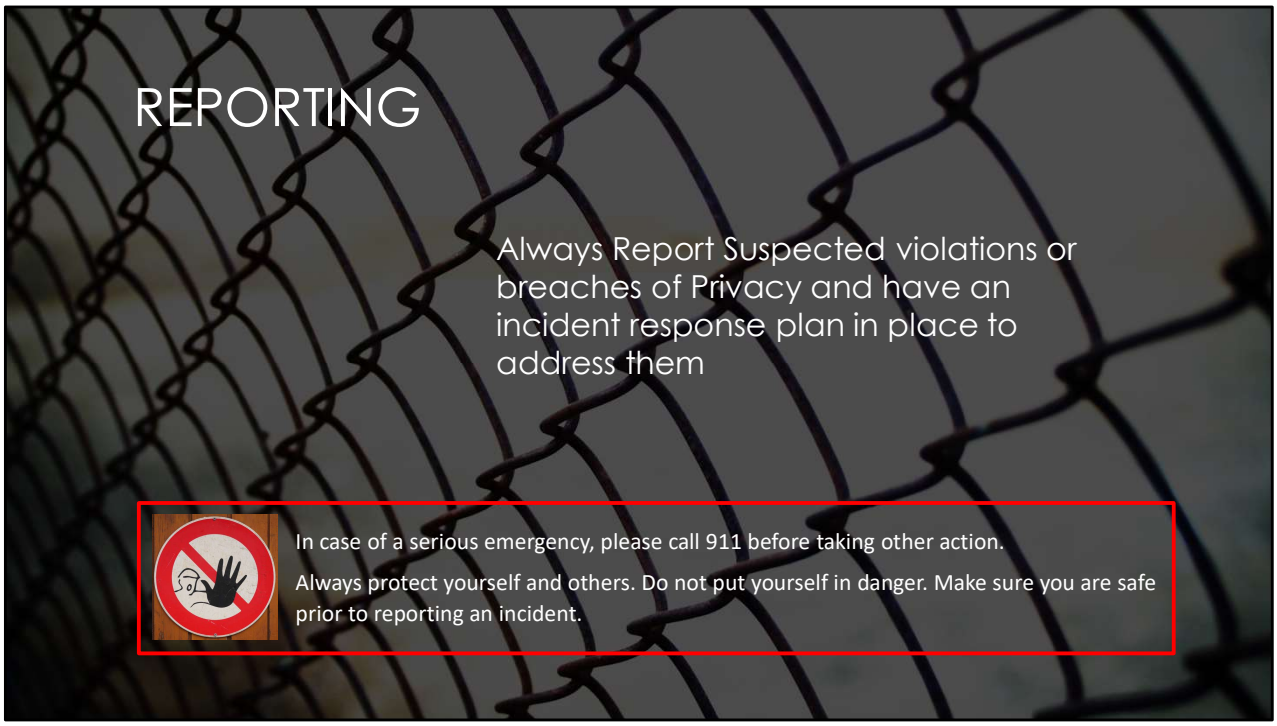
All information should be shared on a need-to-know basis, and even if you have access, you may not have a need to know and viewing the information could result in a breach.

With the decrease in faxed documents and the implementation of secure printing, the likelihood of leaving printed private information on a printer or fax machine is diminishing, it is still a risk.

Protect your devices. Quite often a missing laptop, USB drive, or tablet is enough to be considered a breach of privacy. Certainly, there are technologies that can mitigate risk, but physical security is still key.

Shoulder surfing is a risk. Always protect the view of your screen when working with private data. This goes for printed material as well. One of the cases that was used to define the third-party problem I discussed earlier was related to discarded paper documents. The supreme court determined that you have no expectation of privacy if you throw a document away.

Finally, always read the terms and conditions and end user license agreements. In many cases, the only requirements a third-party must follow to protect your privacy is defined in the documents they wrote.



My institution requires the

- Reporting all lost or stolen assets, including personally owned devices that may contain private information.
- Reporting physical intrusion into secure areas
- Discovery of malware
- Any unauthorized access to information assets , and
- Inappropriately shared, exposed, or lost private information

Every organization has a responsibility to have a clear process of reporting suspected breaches and an incident response plan to follow when a breach is reported.

Finally…

I am glad you chose to participate today.

I have heard it said that people are the weakest link in our cybersecurity defenses. Personally, I don't like to think of it that way. The technology is here to serve you.

You are our greatest resource when it comes to building a culture of security. We are all in this together.

THANK YOU!