Please stand by for realtime captions.

>> Good morning to our physical audience and good morning to our virtual audience. I am from the Catholic University of Puerto Rico. This morning our program is on cyber security and your personal information. I didn't realize what a big thing this is until I was walking off the airplane in the Reagan national Airport and they are like five signs advertising five different companies who provide cyber security I think we have hit on something that is necessary. Obviously for those of us in the library, I think that we are both concerned about our ability to provide open, free, and accurate information at the same time that we are protecting our users privacy. And so that is how this program was born out of our programming in April. With that, in order to give our speaker sometime, I am going to turn you over to Anthony Smith who will introduce our speaker for the morning.

>> Good morning. I am Anthony Smith chief of project systems. Every month is a good month for cyber security awareness. It just so happens, that October is national cyber security awareness month. It is a collaborative effort between government and industry to ways awareness about the importance of cyber security and to ensure all Americans have the resources they need to be safer and more secure online. The focus in 2019 emphasizes the importance of personal accountability and taking proactive steps to advance that. This year's overarching message, own it, secure, protected. We will focus on key areas including citizen privacy and devices and e-commerce. And I am very pleased and excited to welcome our guest speaker Mister James Burd. He is the acting director of privacy at the cyber security and infrastructure security agency system. Within the Department of Homeland Security. He's responsible for protecting the nation's critical infrastructure from cyber threats. This mission requires effective collaboration on a broad spectrum of government and broad-spectrum organizations. Recognizing the mission and statutorily required privacy officer which is a matter of policy is [Indiscernible]. His office is integrating full individual privacy protections into the management of state and resilient physical infrastructure. The privacy and civil liberties information sharing act of 2016 oversees one of the federal government's largest programs. And works with stakeholders across the government and private sectors in efforts to make personal information more secure. Prior to working he worked on biometric law enforcement intelligence and immigration at DHS and data governance issues in the private sector. Clean please join me in welcoming Mr. James Burd.

>> Good morning, everyone. I know it's first thing in the morning. This is your first session and it's very dense subject matter. I want to thank each and everyone of you for attending. I will try to make this light and easy. I would like to thank the GPO. Everyone in this room has a role to play in enhancing cyber security. It is a shared responsibility. It rests on no single person and no single organization. It is a critical challenge. Whether we will talk in the public or private sector. It serves as a private reminder that it is a national issue that needs to be addressed. It isn't something for organizations to worry about. Cyber security is something that is handled by everyone across the spectrum. If you talk about an end-user. Cyber security is something that can be taken into your own personal control. It's not another layer of security. >> I would like to tell you more about the agency. I am from an organization. That being said this is a risky question. How many of you have heard of it? That was more than I thought. Don't feel bad if you've never heard of it. We are a newly established agency in November of last year. Prior to the establishment we were known as the national protection [Indiscernible]. If you don't quite understand that name it's okay. We were working on our long-standing mission to work with owners and operators and private sector and local government to identify and counteract the infrastructure. Particularly adversarial nationstates and state-sponsored organizations. It led the effort for critical infrastructure. This is ensure to us. We are very unique as a government agency. We don't regulate or compel people to

work with us. So what are we? Our sole job is to protect and defend networks. Like many other government agencies there is a specific purpose tied to law enforcement. We have to provide value to the greater community. Again this is not a regulatory action. You have to provide something for people that want to work. We have unique tools and authorities. For those of you who may not follow this specific area we have a term called [Indiscernible]. That means there are a lot of things in our country that are pretty [Indiscernible] relying on our day-to-day lives. Critical infrastructure is systems that are so essential that it is required to ensure the safety of the operation. Back when 9/11 happened, we realize that the adversaries used are critical infrastructure to attack another element and kill people. And the thing was, none of the critical infrastructure I mentioned [Indiscernible] specifically in the transportation area. These were all privately owned. These were things that were simply run-of-the-mill business properties. It forced us to change the way we protect our citizens. A lot of the authorities surrounding terrorism. And counteracting that. Were specifically it was more about that. We increasingly realized it's not just about terrorists who want to attack. Cyber vulnerabilities today are one of the biggest strategic threats to the United States. Those who wish to explore vulnerabilities don't just come from rock. Their enterprises and [Indiscernible]. They are highly organized. People who wish to exploit these vulnerabilities [Indiscernible]. The idea that we must counteract a specific group of people is a little bit foolhardy in the sense that the adversary could be anyone from a person with Mal intent to a person who did not know better. We prefer those who are a little bit ignorant not to be called adversaries but are people who don't know very well. The main gatekeepers of the nation's critical infrastructure isn't the federal government. The vast majority of the infrastructure is owned and operated by someone other than the federal government. Its local enterprises. It's local governments and public cooperatives. It's you and me. The cyber security of the nation's infrastructure falls on the shoulders of the American people. While we really lead this we cannot do it alone. Cyber security is a shared responsibility. We are here to help you figure out how to handle this burden. Let's talk about privacy and cyber security. We talked about protection of personal information. Over the last few years there was an unfortunate movement to consider this to be one in the same. It's born from movements to adhere to compliance regimes set up across the world. There's a tendency to say that. Let's try to lump things together so we can solve them all at once. It's important to remember these are different things. One can't exist without the other. Privacy is described as the right to be left alone. To be free from interference from someone who is not trusted in your inner circle. There is also information privacy. The right to have some control over your own personal information and how it's collected, used, and shared. Cyber security focuses on more of the protection of data and those individuals and their right to privacy. Were talking about protection from malicious attacks or exploitation of data or any kind of intrusion into your own personal and private space. Whether it be via cyber means or physical means. CISA considers the protection of sensitive information a national, critical function. Specifically it can have dire consequences. We actually do consider the personal information that is handled within the various critical infrastructure to be a critical function. In other words, that function should be compromised, this country risks facing a security function or health risk. Our focus is to increase resilience

in risk management and improving cyber security of the nation's most critical systems and function. One of these are known as the nation's federal or.gov networks. For the last few years they have made tremendous progress in strengthening defenses. Cyber attacks are growing more sophisticated and aggressively every single day. I CISA we provide capabilities to departments and agencies in order to manage network vulnerabilities . We measure progress and motivate agencies associated with cyber security and privacy. We also provide operational technical assistance including threat information dissemination and risk vulnerability assessments. Essentially we provide the full spectrum to government agencies with regard to what is the threat and how to handle the threat and here are tools we can use. If you actively phase 1 we will actively assist you to it have it or clean up after the fact.

These activities are not visible to the public. We do this to make the visual services that they provide whether it's at the government level or state level or whatever level to be as seamless as possible. We should never know that CISA is in the background performing cyber security services. Whether you are logging into IRS.gov to submit your taxes or you are browsing the website to find information about activities or if you are simply going to [Indiscernible] a parks they picked these are things you may wonder why is CISA concerned with this quick any front facing portal between the government and public is exploitable . These are things where if a member of the public in accident, a person with nefarious means will be able to access it as well. The services we provide pretty much split the two. We ensure the people who are using these services are able to do so in a seamless manner. At the same time people that wish to exploit them are prevented from it.

>> Despite our best efforts there are certain vulnerabilities we have a hard time protecting against. There is one major vulnerability we struggle in today. The vulnerability is you - - not unique to the government. It's found in hotels and libraries across the nation. It's a significant one. And most people are not comfortable talking about it. The vulnerability is you and technically May. Not shifting the blame but it touches on almost every aspect of our lives. We can shop, bank, and handle things online. Many of us trusted online applications to handle sensitive information. It is involving information. May be we have become numb to it because there were so many reports about breaches across the country that you hear over and over again. Why should I care anymore? What if I were to tell you the vast majority of data breaches are not necessarily caused by a specific vulnerability in an IT system. It's basically exposed due to bad cyber hygiene practices. Whether it is a customer or a person working in that organization. These are not sophisticated actors with complex schemes exposing secret vulnerabilities no one knows about. The vast majority are committed by petty thieves who figured out somehow your login credentials. Let's run with an example. >> There is a rather popular neighborhood app but it's a social media app. It's something people used to connect to their neighbors and maybe gossip about them. It was relatively recently breached and a sense that your login information wasn't properly secure. If a person was able to see your login information they were able to see your username and password. They weren't necessarily able to's see the information in the account or the personal details of your code. That wasn't necessarily reveal. The login information was. By nature, as humans we are naturally lazy in a sense that if we are not given an alternative to make things easier, we will make things easy ourselves. We have a natural tendency to use the same login information across all kinds of applications, tools, and software. Whether it's for our own personal use or the use in the workplace. Often times we find a person will use the same username and password for their accounts. It's easier to remember. When we take a look at that, we realize that if the username and password for one application is exposed we make the assumption that all applications are exposed. The answer to that is yes.

>> To further detail the example without naming different organizations but we have also learned that for the developers of the neighborhood application, there are certain people that are trusted with verification that have unusually high privileges within the organization. We call them low-level system admin's. They are typically admin's that

don't really exist but they are granted to individual people mostly because they want to spread the work around and they don't want to deal with the idea that I will have to grant this person access to special data over and over again. Let me give them full access so they leave me alone. >> What happened was, this low-level administrator had a wonderful LinkedIn account. I explained what company they work for and exactly what type of activities they did at their job. This person became a targeted person. There was no high level of surveillance. It was simply a petty thief who identified an area they were interested in and decided that these people are interesting and it seem like they have access but they are not really high up in the organization when they don't have a role of high-level responsibility. Let me see what I can find out. The thing was this developer also previously worked on games on mobile devices. So specifically this person was targeted by providing a type of app they believed the person would download. Truth be told the person fell for it hook, line, and sinker and downloaded that game. This was while iOS or the operating system on the iPhone had a specific policy loophole that allowed people to track the data communications between the one app and other app. Without notifying you about the usage. This loophole has been closed. Pretty much if you were providing details to one app and providing the same details to another they would be able to share information with each other about the activities they performed. It was able to create a more detailed advertising profile so those apps could provide you with advertising targets. Also a pretty much provided the details of the person's activities and what types of sites they accessed and what purchases they made. Specifically the person that they like to order pizza via a mobile app. That mobile app had a specific vulnerability in that it did not encrypt usernames and password. The adversary was able to get hold of the individuals username and password and it was the exact same username and password for administrative privileges.

>> The adversary was able to access the controls of the neighborhood app and lo and behold they learned that a lot of the information once you enter within the application or the network in which they pull information from, it was free and open. It was unencrypted. They got the information and they had determined that the person that spoke about originally and that was using the neighborhood app in the first place was also another interesting person. They looked up all the usernames and names of individuals in LinkedIn and saw a lot of these people had different interesting backgrounds and some work for organizations that this person was interested in. Specifically a person work for a city government. This person who worked for the government the username and password that was exposed as a result of the breach use the same one for a number of city service systems. What happened was that using the information they proceeded to log into their accounts for that government. They discovered it offered remote access to the system so they can telework. Lo and behold the telework whether it's VPN or using desktop as a service or any of the other virtualized services use the same username and password they used for those accounts. Are able to access the network and it turns out the person who had the credentials exposed via the neighborhood app - - everyone will have to sign a [Indiscernible] after the session [Laughter] lo and behold the person that was exposed, they were a low-level system administrator for that government. What happened was they use that person's privileges to encrypt everything in the network and lock every government user out of the network. Whether it was a vital citizen service or data within the network or any kind of tool that may be used by those employees. There was also a downstream effect. Every citizen who wanted to use them was not able to do so [Indiscernible-low audio.]

>> The current conversion rate last month was something along the lines of $100,000. That municipality paid the ransom. The decryption key did not work. That's a situation that got out of hand in a hurry. I want to make something clear. In the example I gave you, there was not a single vulnerability exposed. [Indiscernible] was this a bad decision by an individual user? This story gives an idea of how humans are exploited by machines. If the majority of people like you and I performed a measure often referred to as cyber high to pick the number of data breaches would dramatically plummet. Basic security measures that would nip this scenario in the bud. There is a handful. One is improving login protection. Not all services offer this. But there's a growing thing called multifactor authentication. This is who you say you are. Use it for email, banking, social media or any other service that requires you to login. If it's an option enable it using a trusted mobile device such as the smart phone or [Indiscernible] which is a small device that you can plug into a machine or phone. Essentially what it is is this is a second factor. When a person compromises the username and password

you are probably able to use it as is if you don't have multifactor authentication able. When it's enabled, the service will thank you for that now they want you to take a second step to verify who you are. This is the extra step. It takes extra time. We have done studies to see how long it takes to go through that second step. It adds a terrible lag. It adds 12 seconds. It takes time out of people's days and security is a major inconvenience. That being said those who are willing to sacrifice this get an extra layer of security that is on their person. A person may be logging into your account from some remote region such as Lithuania or Idaho Falls, Idaho. Anyone from there I apologize. This is a wonderful place and I appreciated it. >> That being said the second step prevents that remote actor from using your username and password. Another one is that if multifactor authentication is not available what's wrong with shaking up your password protocol? Usernames are probably going to be seen across the board. Who wants to remember them? Who wants to remember complex passwords? Here's the thing. When you use the same password across all devices, when you experience one individual breach, everything else is breached. We encourage you that you use different usernames and passwords across the board. You may have heard stories that your password is dead. That the national Institute for standards and technology issued guidance that the password policies they issue to the federal government back in the 1980s was actually futile. The idea behind it was that your passwords should be a bunch of random characters, numbers whichever. It turns out that if it's eight digits and random, it's usually an algorithm that can be figured out. Let's see you expand the field. It doesn't have to be a number and digit. Or letters. It can be a phrase. Right now the way the language stands and I know colleagues working in artificial intelligence would like to differ but the vast majority of adversaries are not working on these processes. Digging out a phrase is incredibly difficult. I encourage you that when something says it has a 32 character limit [Indiscernible] and write a sentence that you can see. Something that is personal to that people won't be able to
figure out. Using your birth city as your password followed by the number one in! Will probably be very busy to figure out. Having a passphrase that is unique to you, would be very helpful. Also if you don't want to go through that and remember a bunch of phrases they highly encourage the use of this but we call them password managers. They are apps you can download to your computer and store it in a secure environment. Essentially all you have to do is remember a specific code for that password manager. Then there's a second factor authentication. There is no password manager that I know of that doesn't have a sec second factor authentication. It will reveal to you what the password and username was. This is a way that ensures if you have a list of those but is not accessible by anyone else. Another thing I want to point out is we advise you stay up to date. What do I mean by that? You don't need to follow the news but what we mean is if you are software updated that security pass that you have been putting off on, a new update is available would you like to install it now? I know sometimes you are stuck for time but that vulnerability
or the policy vulnerability the patch plugs and is something that is important. Mostly because you don't want to scare consumers. They want to be able to plug-in right away to avoid liability. That being said they thought it was important to provide this and say would you like to install this? You probably should. The longer that you wait to install a patch, the more you are exposed. These patches are not always for technical vulnerabilities. They can be there to close policy loopholes. So the IOS example I gave allowed third-party apps to communicate. That wasn't a cyber security risk or vulnerability. That was a policy decision that was ill-informed. They closed that loophole by putting in a road back. I highly encourage whether it is for your own personal devices or devices for patrons or visitors that those machines or applications are up to date.

>> Finally the last piece and it follows into that is keep tabs on the apps and software you are using. Most connected appliances, and devices are supported by a mobile application. The mobile device can be filled with numerous apps running in the background. You never realize that [Indiscernible].

Gathering personal information without your knowledge and putting your identity and privacy at risk. Check your app permissions. Use the rule of privilege to delete what you no longer need or use. If you are not familiar with the rule of privilege it insinuates

that you trust no one. Start with a blank slate. It doesn't mean you should delete every single app on your phone but what it does is that it encourages you to take a look at it. Let's pretend the computer has no applications on it right now. Basically some through the applications to see what they do. Does it tell me what it does with my information? Am I okay with that? I am I even using this app and would it work in the background without me using it? Both iOS and android phones today require all applications to tell you what they are doing with the information. Once you actually inform yourselves on what that information is and how they use it, decide if you want it done or not. If you don't, delete the app. Don't use it on your phone or device thinking I will get back to it. What happens is these apps run in the background and collect your data anyway. Learn to say no to privilege requests that don't make any sense. I encourage you and these are tips that are relatively simple

even though I may have rushed through these. Visit websites like stop, think, connect.org. It's a research site that's currently run by CISA and the Department of Homeland Security and the cyber security threat alliance. It's a private sector organization interested in private sector security. There's a lot of information there that tells you about these techniques. Another good website to visit is our own agency, CISA.gov. You will see a campaign that says get cyber smart. It's aimed at individual end-users. Not just about enterprises and organizations aimed toward people using the devices and the activities they can do to protect himself as was mentioned earlier, the national awareness month campaign one of the key elements was the onus. Own your own personal data. A lot of decisions you decide to make on your own go along way in preserving your privacy.

>> The bottom line to my speech is about how you as an individual can improve cyber security. We are having the same conversations with companies, local governments, schools, nonprofits, and other organizations. Whether it is for the consumers or their own organizations. This partnership is crucial for any cyber security plan. Whether it be through information sharing, education, sharing best practices or assisting when a cyber disaster strikes. Every agency, company and individual show information and infrastructure.

It's a matter of that. Don't worry we have the script.

>> Thank you, James. A lot of good advice. [Applause] >> In case you are curious the current rate for a bit coin right now is $7500. It's about $112,000. The ransom price.

>> What I was thinking was that we make sure we get our audience questions both in person and virtual [Indiscernible-low audio.] Jane and I have some questions. We want to give you all an opportunity as well to ask any questions. Maybe we do one or two. Actually I think James answered some of my questions. I am actually going to go a little off script and give you an example of something that happened to me and from there you can talk a little bit about how - - what the signs are. I am pretty technologically savvy. I work with technology and data all day. I also happen to have moved into the area of one of those vulnerable populations. The elderly. [Laughter] I received a telephone call not long ago which started off, hello, I am John from Social Security. I need to tell you that we are about to suspend your Social Security number. Your information has been breached. I know better. I almost answered the guy and I know better. I know the Social Security agency is not going to cancel my Social Security number for any reason. But he was so sincere and so close to convincing. That I almost said tell me what to do before I realized and at that point what I did was hang up. I think my question is twofold. What should you do you handle that kind of telephone call or something you may get on the computer that may be similar? How do you recognize the signs that you are getting something on your phone or computer that could be fraudulent and deal with it ? >> The first thing I want to say is something that is a little bit laughable in the sense that if a government agency is coming to about yourself they will come to you with as little info as possible. They will tell you somethings wrong with your so security number.

They probably wouldn't even go that far. They are going to make every single approach to contact you via alternate means. To verify the identity. So having a phone number on file isn't really a means for a government agency to say this is James [Indiscernible]. Oftentimes you will see something come registered mail. It will say we've noticed there has been a problem with your file or your account and we would like you to contact whatever reference number. They make you come to them. As opposed to them coming to you. For government services that can be a problem. For the most part the information they convey will be detailed. We see the same thing across other sectors. For banking information we received a phone call saying there was illicit charges on their bank account. Essentially what they come to you with is they tell you the problem but before they tell you what it is they verify who you are. They verify who you are and they start providing you with information that only you really know about. If a person is taking guesses they may answer questions incorrectly. If they are unaware of certain things they will react in certain ways. [Indiscernible-low audio.] they will verify who you are. There's a lot of steps that occurred with the actual statement of there something wrong with your bank account. If you ever find that and they are coming at you with a statement or threat.

>> I am really intrigued with the whole concept. I think as you described your agency doesn't have any regulatory authority or oversee
this kind of arrangement. [Indiscernible-low audio.]

>> One of the most wonderful incentives is [Indiscernible]. No one likes being sued. No one likes being sued. What's happened in the last 20 or 30 years is that a lot of security tax are due to what is explained or lackadaisical security practices. Once a company is found to be viable for the inability to provide that. Because of that, as an organization we offer framework and we work in cooperation with other agencies who have framework. We inform organizations that these are the types of things you can use to decrease your liability. Working voluntarily with us, we are able to take a look at the function and give you advice on the different loopholes or vulnerabilities you may have. We won't tell them they have to do things one way or the other. That is not a place for the government to have a private enterprise doing their day-to-day work. There are other elements of the government that look beyond cyber security to see what they are protecting. Let's take the FTC for example.
They take a look at consumer affairs and commerce and trade actions. They are really there for protecting the consumer. That being said it was because of a vulnerability that a person's trust or consumer affairs was exploited the FTC will go after that violation. Another example would be the Department of Transportation for the purposes of safety. If a smart vehicle or vehicle with a smart device on it becomes compromised because of a hacking vulnerability let's say gas pedals can be accessed or something along those lines. Transportation will after them for that. There's really no agency that will go after you for [Indiscernible]. Cyber security is just one means of protection. It shouldn't be a means for enforcing a specific protection regime. But enforcing the protection itself. What we do is we provide a mechanism for private entities to say we understand you are responsible for this part of your sector. We have framework available that we can teach you and get you to learn. It will lower your liability risks. >> I just want to encourage you all to jump into the conversation. Feel free to step up to the mark for the mic.

>> We have a few audience questions. >> Sarah Erickson University of Florida. As James example illustrated one thing that they do very well is
programming. Is there any sort of programming that we could tap into that you guys provide to help spread the word about being more aware of the ways to be more secure with your personal information and cyber security? This is national cyber security awareness month. As one of our campaigns we do as part of the federal government to inform the public about cyber security. This month alone isn't the only time people should worry about it. I mentioned stop think and act.org. It has a lot of resources and educational materials and something as simple as posters. They linked to various organizations including

the ACLU and they provide posters and education materials free of charge. One of the most common things we see that is highly effective is the poster.

So typically when you have that poster and it talks about something that someone deals with on a daily basis they are encouraged to learn more about it. These posters have reference materials. We also offer pamphlets and other items as part of awareness month. [Indiscernible-low audio.]

>> We have regional offices all over the country.. They are not just cyber security issues but [Indiscernible]. One thing I neglected to talk about for CISA is [Indiscernible-low audio.] >> Does CISA produce any public-service webinars ?

>> Yes if you go to CISA.gov you will see announcements about public webinars. You will find links to a website.

>> We offer the virtual training [Indiscernible]. Which was a catalog and training resource if anyone wants to learn about a issue.

>> Vanderbilt University. One thing with privacy and apps that I run across are the privacy statements. And what they do with data. What I find is usually they are about 40 pages long and I am by no means anything resembling a lawyer. I don't necessarily know what someone is going to do with my data. What can we do to combat that? Is that a sign that I shouldn't use this service or do I need to go check with a lawyer every time I want to download an app? What can we do to secure for citizens?

>> If an application provides you with simply a 40 page privacy statement or end-user licensing agreement, and doesn't provide you any other information it's a good sign you probably shouldn't use that app. Mostly because they are bearing you with information and they would rather you not understand what they are doing with your information. The reason why I say that is because there are mechanisms out there we have seen private sector entities use to be as transparent as possible. Those privacy statements are necessary. We told you about every single detail. It wasn't our fault you didn't understand it. Those are called plain language statements. Statements written in plain language for this. They allow you to access the privileges or settings within those applications to turn things on and off. They say thank you for reading our privacy statement. If things you don't understand we have a book or guy that you can read that may be 8 to 10 pages that has graphics and simple language and will explain what we mean by certain statements. That being said those companies that do that they are good stewards for project the image. The trouble with that is making sure that the plain language statements and there may be a gap. It's an
approach we see that is moving forward. Also the environments where they are hosted are taking manners into their own hands. This is a company that does privacy policies. We know that Google has made some basic effort with your talk android or Google Chrome and telling you that this app does X, Y, and Z. Do you want to grant them permission to do that?

>> They don't tell you why that's where it's important for you to Rees those plain language statements they will tell you exactly we know this setting we want to monitor the location here's the reason why we are doing that. It turns out it is a public safety app that allows you to hit a single button to tell someone where you are. Maybe it makes sense that it tracks your GPS location then. Then again if it's a game where you are matching up [Indiscernible] why do they care about the location? I can tell you why. It's usually because they can tell your region and how long you spend on the phone. To see if you're interested in the activity. They see you are playing this game in a retail store and they say this person has been playing this game but they are not shopping around they are providing metrics and information saying they don't like what you're offering that's fine but is it something you are okay with? Are you okay with the app sharing information with that person? Do you want someone else to know about your shopping habits? You have a right to say that's not something I want. If an app doesn't disclose those activities, and you have to say don't trust us we are only monitoring this information. It's

probably a sign not to trust them. >> You started to get to my question talking about why they do it. I am something resembling a lawyer I have a lottery but I am not a practicing attorney.

I do tend to read as much of the privacy paperwork as I can

. When it gets to be 40 pages on my phone I tend to skim. I do tend to turn off location services when I don't need them. What I lose is the why. What I miss in the policy is what are the red flags what I want to know is I can see what they are doing but I don't know what's problematic. I can see what they want and figure out why. As a non-cyber security expert I can see - - I might be able to make a judgment about what the law allows. I don't know what is problematic in terms of security. That's what I don't know. I can see that's a problem legally or I don't think you could actually do that. I don't know what's problematic in terms of security. That's where my knowledge Is. You mentioned the

CISA.gov resource. Are there cheat sheets? These things are red flags security wise. The model I am thinking of and I'm not sure if you're familiar with these but the creative comments and copyright models where they have the big symbols and the translating copyright models in terms of plain language. It's like share alike or open sharing models for copyright. Does that make sense?

>> There have been attempts made for the creative comments model. One thing I encourage you to do is open a free app. Specifically one that advertises that. On the advertisement you see that on the corner that has the letter I on there. It's many advertising networks that came together to propose to give knowledge, information, and control. If you click that what will happen is you will go to a webpage and that will tell you all the different organizations or companies tied to that network. They will give you the opportunity to opt out.

What happens is that [Indiscernible-low audio.] some of you have seen cookie banners. It will say not okay or okay. Right now the implementation is on that. That being said it's just one framework there really isn't a universal framework for software. The EFF or access now organization has a cheat sheet on what to look out for for policy statements. If you sign up for a free service but we have to understand is the ability to make that service free is not necessarily your usage of the service at the information you provide. Because of that your payment is not something that is tangible or physical it is the information you provide. They will use that information for various purposes. One thing we look for in a privates statement is to look at the third-party disclosures. If the section is simply two senses saying they may share the information with advertising partners to better determine what kind of products they advertise that is a poorly written statement. And certain regimes they are required to identify all the different companies and organizations they are sharing that with. Or they are required to say how the activity takes place. They will provide a link to that framework. They are not open and upfront as to who they are sharing information with beyond themselves. That's a significant security problem.

It's one thing if you trust the security organization you interact with but if there's a third party and you don't know who they are or what they are using it for our how they store data, that's where they see this. The major data breaches we see are not what affected but who they contact out to that has the data breach. >> We have a virtual question. >> This is a series of question. I know we are out of time. Can you say anything about the call for one identity or identity verification for social media and how would it be enforceable? What is the downside?

>> First and foremost I am a privacy officer and a privacy advocate. One of the basic concepts of privacy is to be able to express yourself freely but anonymously. One thing about having that is that if you're identity is tied to it you may curtail your ability to express yourself. If you are shedding light on something that you feel you have retribution for that is very powerful and helpful. That information may never see the light of day. >> That being said the idea behind having one identity on the social media platforms is the idea that there are a lot of people that will pretend to have this position that they don't actually have. They give you the idea that I am an authority and they may be worse in representing themselves. They may be terrible things tied back to them that will affect them in their workplace or personal life. There's a lot of value in that. Brings on the idea of responsibility. There's a bit of a

balancing act that has to occur. One thing I would encourage is not to forget about the power of making an anonymous statement. Accountability is important. I don't think this is a this or that conversation. >> We have run out of time. I want to personally thank you all for your interest in this topic and for all the great questions today. James I want to especially thank you for your expertise and for being here to share some of that. >> [Applause] >>