[Please stand by for realtime captions.]

>> Good afternoon everyone. Let's go through a few housekeeping. You can download slides and handouts from FDLP.gov on the main homepage right in the center there is the large spring meeting banners just click on that and you can get the handouts from there and if you have questions or comments enter them in the chat box bottom right-hand corner of your screen and once each presenter is finished with their session we will relay the questions to them. We are also recording of the entire meeting and once this meeting has ended you will receive an email with links where all the recordings are and slide and handouts and a link to our event survey which we will be very pleased if you complete that for us. Follow along on Twitter, the virtual -- I will hand it over to Jim to get us started.
>> It is Anthony Smith. Hello everyone. This is Anthony Smith and I'm here with my colleague, Jane Canfield and I want to thank you for attending our session titled security information protecting privacy providing access legal constructs and library impacts.
What we are going to try to do with the limited time we have because we have a lot of information to share is I will try to provide a general overview and history of the topic. Jane will provide a closer look at how privacy has impacted our profession but thirdly we hope to be able to spark some interest in deeper exploratory discussions at future FDLP events or other events. Let's get started.
>> It's the philosophers who establish a foundation for the concept of privacy. The Stanford Cyclopedia philosophy describes privacy is something that is interpreted and then applied differently by different individuals. Legal scholar Alan Weston said
, in 1967, values so fundamental to society as privacy have been left so undefined in social theory or have been the subject of such vague and confused writing by social scientists. The privacy theorist Daniel Solov said privacy is an -- in disarray. In his book Charlie Sciec said privacy is like oxygen. We appreciate it only when it's gone. But it was in 1890 Harvard Law Review by Samuel Moran and Louis Brandeis that established the modern concept of privacy. The two make the case that privacy is an individual right that protects against social and technological pressures of the time. What exactly were some of these contemporary pressures of the time? In her book the known citizen, a history of privacy in America, Sara Igel describes the Victorian Internet. A phrase first coined by Tom but in both cases the late 19th century is described as a significant period of time when new technology was challenging and citizens right to privacy. They wrote about the impact of society pages in the newspapers industries, interest in the sex lives of individuals. They also describe the major implications of instant photography where images are freely circulating without the consent of the subject. And as the telephone and telegraph became more economical and more common, wiretapping became a central concern in popular culture. Standards writes today the Internet is often described as an information superhighway. It's the 19th century precursor, the electric telegraph was adopted the highway of thought
. Modern computers exchange bits and bytes along network cables, telegraph messages were spelled out in the dots and dashes of Morse code and along wires by human operators. The equipment may have been different but the telegraph impact on the lives of users were strikingly similar to today. Of course we cannot have a conversation about privacy without talking about the impact of data. In 1880 the U.S. Census office was struggling with how it was going to tabulate census results for 50 million people. Manual processing of the 1880 census would take almost 8 years and census made 11 years for the 1890s making it obsolete before the results could be reported. They started working at the census office in 1879 and was inspired to solve agency dilemma and decided to take on the challenge. The use of electromechanical automation technology was the gold and in 1884 color it's received a patent for the first punchcard tabulating machine. The photo on the left is an example of his first punchcard tabulating machine. The device that fits on the desk on the left is actually the coding equipment that the operator used to punch holes in the punchcard after transcribing from the actual census form and then

the device that is sitting on the desk to the right is actually the card reader unit, which actually reads where the punches are and updates the dials on the display. It was put in service with the 1890 census which by then, the population had grown to 63 million. I read somewhere and I need to verify this that it took three months to tabulate 1890. In 1896 he formed the tabulating machine right here in Georgetown. The company was renamed in 1924 to the international business machine corporation or IBM. Fast-forward to the second half of the 20th century when Peter -- coined the phrase democratization of personhood.

To describe social political climate of the 60s and 70s the rights of individuals were being championed on many fronts. The civil rights movement was accompanied by the women's movement, there was protest against mandatory draft for Vietnam, process -- protest on behalf of Native Americans and outspoken voices calling for the right to privacy. In 1965 Griswold versus Connecticut was established modern right to privacy in the U.S. when the Supreme Court ruled in favor of protecting the privacy of married couples and their use of contraceptives. Justice Douglas who served on the Supreme Court at the time describe the decision of the case is one based on values that predate the Constitution. This case was quickly followed by loving versus Virginia over overturning the ban on interracial marriage and the position of materials as a private matter and of course Roe versus Wade. Also in 1974 Congress had expressed concerns with curbing legal illegal surveillance of persons that have been invaded during the Watergate scandal and the was concerned about potential abuses presented by the government increased use of computer to store and retrieve personal data by means of personal identifiers such as Social Security numbers. That same year the privacy act was signed into law as a way of balancing the governments need to maintain information about individuals and protecting the rights of individuals from unwarranted invasion of privacy's collection, privacy use and disclosure of personal information. Here is a few concepts part of everyday life. Where information sensitivity receives our attention. Where access controls and rules must be established to protect individuals and organizations. What I did not list, and I thought about this after I had to submit my slides, is personal concern for a growing number of us for DNA data. In the digital space. The genetic information nondiscrimination act signed in 2008 provides some protection against discrimination by employers and health insurers. There is still apparently some debate around other life insurers can use genetic information. The national notification and information administration is leading the Trump Administration effort to establish policy for consumer data privacy. According to assistance secretary Randall a TIA put out a request for comment and received more than 200 responses. He provided three overarching themes from the responses that he received last month. There appears to be a sense of urgency for national privacy laws, number 1. Number 2, respondents did not seem to favor a patch word regulatory landscape within the U.S. And third, there was strong support of the NIST privacy framework which I will talk about briefly. In Congress Senate Bill 142 was introduced by Senator Rubio on January 16th of this year. It uses essentially the privacy act of 1974 as a framework. Also a bipartisan Senate bill 189 was introduced by Senators on Jerry 17th title social media privacy protection in the civil rights of 2019. This bill would give consumers the right to opt out and keep their information private by disabling data tracking and collection, provide users greater access and control over their data. Require terms of service agreement be in plain language and ensure users have the ability to see what information about them has a ready been collected and shared . Mandate that users be notified of breach of their information within 72 hours. Offer remedies for users when a breach occurs and require online platforms to have privacy programs in place. Some states like California, Utah, New York, are modernizing their state laws. New York introduced a new bill on Jerry ninth, and the bill gives consumers the right to request personal information that has been collected by companies and is being disclosed to third parties. On March 27th, Utah's governor find the electronic information or data privacy act into law. This new state law requires law enforcement officials to obtain search warrants in order to access a person's data that might be held by third-party service providers.

>> I just wanted to go through a quick list of some of the privacy laws enacted since the 60s and I am going to go through these rather quickly but I wanted to point out a few things for you. FOIA gives the right to request certain records and as part of the privacy act federal agencies are required to issue system of record notices in the Federal Register for any system that maintains personally identifiable information. The privacy protection act of 1980 was put in place to protect journalists and newsrooms from search by government officials. Each year

as some of you probably can relate to this, my daughter's school has to sign a consent form indicating whether we do or do not grant permission for the school to include photos of our daughter in its newsletter and website. And this falls under the children's online privacy protection act of 1998. The U.S. patriot act, I never knew what that acronym stands for. Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism act of 2001, for those of you who did not know. This data you cannot see on the slide. It is a state side-by-side comparison

of privacy laws that are currently enforced. California scored the highest on this particular comparison based on 19 metrics which are indicated but I really wanted to show you the green versus the red. These 19 metrics that are there, California is the 5 from the left, which has the majority of green of any state . California's consumer privacy act, was enacted on June 28th 2018 due to come into full force January 1, 2020, CCPA has some align -- alignment with the EU GDPR. One of the differences is that CCPA includes exemptions for small businesses with less than 25 million in annual growth revenue or those that collect personal information from fewer than 50,000 consumers or derive less than 50% of revenue from the sale of personal information. One other thing I wanted to say about state law, during his testimony before Congress in March, David Hoffman of Intel stated that there are 94 other privacy laws at some point or state privacy laws at some point in the process of discussion and introduction so there is a lot of activity. This table, it was extracted from the international telecom survey data called the global Cybersecurity index, GCI and it's based on five pillars they used to determine a country level of readiness regarding Cybersecurity. Those five pillars are legal, technical, organizational, capacity building, and cooperation. Many at the top of the GCI were EU countries. The U.S. is number 2, you cannot see that up there. This is a good place I think to mention the European union general data protection regulation or GDPR which became a law last May and applies to organization inside or outside of the EU transacting with any EU citizens. Here is some things that are included in the law. The organizations that breach data protection requirements can be fined significantly. Under GDPR companies can no longer provide long illegible terms and conditions that are not easily understood. A data breach must be disclosed within 72 hours after becoming aware of the breach. Citizens have the right to full access upon request. EU citizens have the right to be forgotten. EU have the right to be forgotten. Privacy by design. This requires system operators to build in privacy controls during the development phase. This includes data minimization which NIST also speaks to in its framework. NIST states on their website that the framework is being developed to help organizations better identify access, manage, and communicate privacy risks. It also seeks to foster development of innovative approaches to protecting an individual's privacy as well as increased trust in products and services. Here is sort of a quick timeline on where they are in the planning and implementation of the framework. They released an RFI last November, November 2018, in between November 14th and January 14th of this year they received 80 responses from that RFI. There is a workshop scheduled next month, May 13th and 14th at Georgia Tech and registration is still open if anyone is interested. It closes May 6th, if you're interested in participating in that discussion. They are planning to make available the discussion draft sometime in May which I'm assuming will be after the workshop. Let's talk about Internet of things. When I saw the headline last week, Amazon workers are listening to what you tell Alexa. I was sitting on the sofa and she looked at me and said that is creepy. And then she reached around because the sofa is right behind us and she unplugged are smart speaker. Because she uses Alexa. Later that day I found the full story online.

Amazon says that and this is quoted from the Amazon representative, we only annotate an extremely small sample of Alexa was recordings in order to improve the customer experience. For example this information helps us to train our speech recognition and natural language understanding system so Alexa can better understand your request and ensure the service will work well for everyone. The article also provided some instructions on how to opt out of their sampling to which was helpful for me because I do not know how to do that but I do now. The number of estimated IoT devices in 2019 is 8.3 billion and is expected to climb to 21.5 billion by 2025. What will this mean for privacy by having all of these sensing devices everywhere? HR 1668 IOT Cybersecurity improvement act in 2019 was introduced March 11, 2019, last month . It provides guidance on oversight for the government implementation and use of IOT devices. Also as part of CCPA California will require and that was one of the greens at the bottom , California will require certain -- entitled in the state beginning January 2020. Looking at ahead, what are some things to pay attention. Like artificial intelligence, it's already here although I think most would agree that we are only at the very early stages of integration of technology in our society. I spent the last 29 years gathering data about my ancestors. People who lived long before I was born with the goal of analyzing the data in this is mostly public records, that's the traditional legacy way of doing. If I spring forward let's say 72 years, what tools will family historians have at their disposal? I am going to venture to say that it's likely they will have AI and access to the digital data footprint about me and others of our generation to work with. What is contained in that footprint will depend on the direction right to be forgotten, laws of the future, it could be the usual public stuff the record is court record. What could be more? The deployment of 5G, LT replacement has ready begun and promises to significantly increase higher bandwidth but more importantly to IOT is ultra low latency which will allow sensing devices to receive and react to events at rates far closer to real time then LTE. Latency rates are a critical characteristic for some functions such as autonomous driving. Transmissions can respond and they need to occur in rapid responses. It also means that a smart vehicle no longer needs to rely solely on its own sensors. It can interact and communicate in real time with other vehicles traffic wide and the road etc. and make the necessary adjustments to maintain safe operations. Just an example of the significance of this. A connected car traveling at 75 miles an hour with travel over 10 feet further before applying the brakes if the system was experiencing a 10 millisecond delay. For those who are not familiar with

block chain, it's a way to record encrypted transactions metadata in a digital ledger that is distributed, replicated, using peer-to-peer networking. It is great for detecting data breaches however, due to its public nature, the privacy is not its strong suit. According to fire I Cybersecurity vendor it takes an average of seven months for an organization to detect a breach. For block chain detection its immediate. To address privacy there are efforts underway such as MIT's enigma project which is developing a way to build an additional block chain layer to essentially manage data privacy. It does so by establishing a protocol that prevents any single note to ever have access to full data, referred to as secret data. Instead of it being divided among many nodes and relations are performed in a distributed way so no note ever had knows what it has are fully calculated on. Finally, we will certainly want to keep an eye on the development and quantum computing. I would love to turn this piece over to a PhD in quantum physics, and if there's any other room but I'm going to give it a go. A classic computer we all know how that functions. It's the principle of two binary states. It's light on, light off analogy. And the way complex calculations are performed it's stream together the series of binary state or bits to perform those complex calculations. Quantum computing is completely different. It is not a faster computer than the classic, in the classic sense. The analogy I have seen in the literature is the candle to light bulb. It's a whole different way of lighting

the function of providing light. Basically it applies to laws of quantum physics and superposition and what it does is it tries to harness the behavior of Adams -- atoms in the way quantum computers process information. Instead of only two states, the quantum bits can be either state or any combination of the two states. If you are scratching your head right now, you're just fine. Your right where the rest of us are on this. The implications of quantum computing are significant with regards to problem-solving. Like most technologies can be used in ways that are culturally constructed or destructive. I think many of us can get behind the promise of finding out how to conquer cancer. At the same time we must also pay attention to uses of the technology that can do harm. For example it's believed by many technologists that quantum computers will have the ability to break all the encryption that's currently in use. The bright side of this, not to paint a totally dark picture, is that quantum technology can provide us with new encryption capability that scientists are saying will be unbreakable. Unless you are somehow able to defy the laws of physics. Each and every topic I have tried to cover I think here today is a symposium in and of itself. My goal today has been to provide a landscape overview. The next two slide just provide a few references if you want to delve more into some of the resources that I talked about. With that, I am going to turn the microphone over to Jane. >> Good afternoon. Now that Anthony has given us a look at the past and a look into the future, I want to talk about how the issues of privacy security and access are affecting us in serving and protecting our users. I think all of us are aware that sometimes these are conflicting issues and how do we provide privacy for our users and security of information and at the same time provide access to information. Want to give a few statistics that I came across an if you research report. They're very telling about how we, as Americans deal with online security. 64% of us personally experienced a major data breach. I can put it partners -- personal example. Our older son had to change his Social Security number after his identity was breached and he found out about it because he did not receive a federal income tax return that had been sent to someone else. I would say that 64% of us may actually have gone up since this report was done. 41% of Americans in this survey said that they have had fraudulent charges on their credit card. I know that recently the two banks I deal with in Puerto Rico started sending out alerts every time I make a transaction , I get an email or follow-up alert that says -- the most recent one I got one that says you're out of country. Are you sure this is you? So I think there are measures being taken to combat some of the. 60% of us -- 16% of us say that somebody has taken over our email account at some point. We have as Americans in general a lock of confidence in data security. I think this report was 2017 I suspect with many recent occurrences, there are more and more of us who feel like we cannot necessarily trust the security of our data. We lack faith in both public and private institutions. 28% of Americans who answered the survey say that they are not confident that the federal government can protect their personal information and keep it safe and secure. I think that has a lot of implications for the Census Bureau data. For instance that we work with 24% of those of us who use social media do not have any confidence at all that our social media sites can protect our user data. However, within that context, most of us fail to follow and this has applications for us in libraries both personally and for our users. We fail to follow best practices in how to keep information secure.

65% of us say that either memorizing or writing down on a piece of paper somewhere and as I -- the picture in my head was the little brown notebook that I carry around that has all of my passwords and bank account information in it, so I am certainly as guilty as the rest of us. 41% of us online have shared our passwords with a friend or a family member. Everybody in my family uses the same Netflix account. 39% of us use the same or very similar passwords, things like the names of your dog or your cat or something that is easy to remember which security experts would tell you is a really big no. We just have policy can implement it at our university where we are now being required to change our password every three months. We are supposed to use something that makes no sense to anyone else like we are not supposed to use our pets name or children's names or whatever so one of my colleagues used I do not want to change my password as her first attempt at this. 12% of those of us who use the Internet, only 12% of us only ever use password management software which is what all of the security experts say that we should be using. That we should all use some version of password security software and I see people already -- obviously we are generating discussion because I'm seeing things in the chat box already which is great. That's our intention today, to get a discussion going. There are impacts and challenges for us. Look at the gate, please look at the gate on this quote. It is from a 1991 article. Librarians must be aware of the pitfalls that can be encountered in collecting, organizing, and disseminating information. We must recognize the lines are not as clearly drawn as we would like for them to be. It would be really nice if I could say, this is what has to be private and this is what is fine for us to access but it is not that way. It is much more complicated. There exist a fundamental conflict between society's need for information of many kinds and the individual right to privacy protection. I don't think this quotation has changed since 1991. It's an issue that, in fact, has accelerated and has been growing for all of us. A little bit of history and I'm going to concentrate on 1970 because 1970 was a apparently a really pivotal year in which a number of libraries were asked by specifically the FBI for information on their users, and this is how different people reacted

. Apparently because there were concerns out there about people building bombs and libraries giving that information, the FBI started asking for user records and the response was varying depending on the library. This is obviously an issue that we have not reconciled as exactly what needs to be private and what does not need to be private. In Milwaukee the city attorney went, public records, give them away. In Atlanta the public library said show up with a subpoena. The Seattle Public Library released circulation records when the FBI did present a subpoena in connection with a forgery case. And the Alamo, Texas, the library said no way, we are not going to do this. We are not going to comply with you at all. Obviously we don't necessarily agree in libraries as to how private our information is to be. And I noticed in the chat box someone put in the link to the American Library Association has recently strengthened its policy on patron rights to privacy of their personal information in libraries. Let's talk about what privacy is and Anthony also defined some of this. Library privacy in terms of libraries is a philosophical and illegal right. -- and a legal right. It does not just involve our personal use information. It's also how we protect what it is they are searching for and in today's world of the Internet usage at the ease of recording digital data, how we protect what our users are searching for and allow them their right to search is important. For libraries privacy is more philosophical than legal. As librarians we do not share the same right of attorney-client privilege, of doctor/patient privilege, that does not exist for us. There is no such thing as librarian/patron protection.

So if we are refusing to release information when it's asked for, we could be putting ourselves and our patrons in legal jeopardy and I think that is food for thought for all of us.

Obviously our digital technologies have posed new challenges to the question of how do we offer free access and at the same time, protect. Protect our user personal information and their right to search for information and the bomb example is sort of a classic in that you may ask me for information on how to build a bomb and you may be a researcher who needs that information. You may not have any intention of building that mom. I think the issue of protecting our patrons right to search for what they want to search is a critical one. How patrons perceive their privacy in the library is important. It's important to their feeling that they can openly and freely access information. Again, I have an example here. In my library we still have two areas that ask people to fill out a paper form which includes your name, your student number, what year you are in, and whether you are using the Internet or whether you are using a Microsoft office document, what course you may be looking for, what professor. Those pieces of paper have been around for probably 30 years with the same information on them. On two recent occasions on Saturday afternoon I had to -- two graduate students simply say that's not your business. I have the right to use the library without filling out this information. We are now as a library involved in a discussion as to what we legitimately have a right to collect and what we do not have the right to collect. I pointed out to both students that as soon as they gave me their student number, in order to enter them into the system, I have access to significant information of theirs and as soon as you are going to a computer, what you're looking for is being recorded but those two incidences have caused us as a group of librarians to start looking at and questioning how we do, indeed, deal with our users privacy and right to access.

>> Security. We should be better at protecting security. We should I think be advocating for our patrons privacy. We should also provide information about if there are existing threats out there that we know about. We should be educating, raising awareness of what the issues in cyber security and privacy are and communicating those to our users. Access, this is a quote from 2010 so not quite as old as 1991 but I think it is where most of us as librarians come from. Core values of librarianship. They include free and easy access to all information for all persons. The importance of preserving the cultural record, the value of exposure to new and disturbing ideas in democracy, innovation and individual freedom and the societal benefit of providing a safe haven for private learning about history, politics, religion, health, science, and art. I think most of us who are librarians would say this is indeed the core of what we do and it is not always compatible with us even being personally attuned to security issues. And I'm going to give you an example that came across in my reading. John Doe calls up a public library and says to the person at the desk, hi, I am John Doe. I am not sure you have the correct information for me. I have recently changed addresses. I suspect many of us would go okay, give me one minute and I will call up your data. You now live at 1921 Pacific Avenue and your phone number is X and we would not even think about that as being a possible security threat. From a security experts point of view we just got hacked at the library. The appropriate answer to that question is sir, would you please give me your information and I will verify if we have the same information. Food for thought and how the everyday little things we may be responding to make us vulnerable to security threats. And Anthony already mentioned this, the right to be forgotten. The concept in European privacy law that you have a right to have your personal information and what you have searched for erased. It has been ruled by the European courts that search engines, even those that are not located within Europe, have to comply with this. This has affected I think all of us in the sense that I have recently received when this went into effect that email, that thing when you hold onto database that says change your privacy settings and your being asked what you want in terms of privacy settings. That has come directly from this European law. There is opposing viewpoints to this and Anthony touched on this talking about his ancestors. Historians and archivists are concerned that if everyone erases their digital information and exercise of the right to be forgotten, we may be losing information that is important in the future. In terms of history. What are some best practices that we can follow, and I'm not going to embarrass anybody by asking how many of you actually do these in your libraries. Encrypted Wi-Fi instead of open Wi-Fi. We do this. Clearing all patron data after every session. Disabling what is known as -- software and i'm not an expert in this but -- software is the idea that when you are logged in and you're using a site, that many companies and Internet sites run in the background a program that is sending your data off to another server where they connect data. This is the thing that enables you, if you just bought something from Amazon and you log into the New York Times, you get an ad for the same thing you just bought on Amazon. That's what this particular feature is doing. Keeping all of your software, particular things that are add-ons, regularly updated on your public computers have they do not track settings set for maximum privacy. On your own line that supplies -- applies to us as users and to us as organizations entities. Make sure your modeling best practices on line. Including send your emails in Safeway's and safe practices. Make sure your checking on your social media presence. If you have social media accounts, it's a good idea to monitor them and not just leave them and not use them and be aware of social engineering. Social engineering is the practice I just cited about the phone call of being receiving a call or getting an email that is designed to make you think it's okay to give this person information. One of my colleagues got a call recently from someone claiming to be from the Census Bureau asking for information. Because she knows me and has been to some census workshops, she got off the phone and she called me and said, the Census Bureau does not call people. That's right. The Census Bureau does not call you. So they called and they said they were from the Census Bureau and they were looking for

information and that practice is called social engineering. A little bit of conclusion and then we will open this up to answering questions and discussion in the chat and hopefully with the idea of this will be something but we will continue into the fall conference as well and all of us are entitled to freedom of access. The freedom to read text and images and expression and these freedoms cannot survive in an atmosphere where library use is monitored and individual reading and library use pattern are made -- without permission. With that, I have included references where I got information from and with that we will open it up to any questions in the chat box and to a discussion.

>> A lot of interesting comments. >> This is Kiersten from the library of Ohio. What you think about situations where the patrons would rather not have their privacy protected? We have run into that for patrons are disappointed when you don't keep track of the books they checked out because they want to make sure they did not read something again because we encounter that -- I have encountered that in the past so I'm curious as to what your thoughts are? >> I did not include that in a presentation but there is some literature out there on dealing with exactly that situation where people do not want their privacy protected. The information I read said that in those cases you can set up and make exceptions for those patrons who don't mind. If you don't want your privacy protected you have the same right to say don't protect my privacy and as you say I want all of my privacy protected.

>> I have a similar question. I was wrestling with how to define privacy and where to draw the line respecting patrons privacy. It was responsibility of mine at my previous job and it is current job to collect metrics around user behavior in my library different web services a website discovery platform institutional repository mobile app. Now how we collect information about user behavior on the platforms is my server, I open a session and then I track them
 and their behavior on my website and this is like a form of surveillance. It is anonymized to some extent but you're still following the IP address of the individual which, if you put all the information you know about the IP address, you can get to the identity if you work hard enough. This is a common convention of just maintaining websites. I'm sure -- does the same thing.

>> Absolutely. >> Though it is conventional I ask the question is this acceptable and
 I'm properly respecting my patrons privacy just to collect this information and of course I'm not doing it for any nefarious notice. I'm doing it to improve the services I provide to the patrons but you could say the same thing about Google. They collect user information so they can ostensibly create a better product for users that advertises more effectively. We are doing something analogous. Should that be an acceptable practice? Where do you draw the line for collecting patron information? >> This is Anthony. It is, that's industry standard practice today. Most institutions that maintain websites by default to collect statistics and data on site visitors but as mentioned it has been perceived as an anonymous activity. We don't necessarily know or equate an individual with that and I can certainly see where at some point someone could, who wanted to do something nefarious, could do some triangulate all the data where they could actually identify an individual. I think and I just wanted to comment. If we go back to the late 19th century, even the things that were of concern over 100 years ago, they have not been resolved. We are still dealing with those things today and two points I wanted to make and one was to the previous question. Because I think privacy is almost like a religion. It is personal and we all come to it from a different perspective on what it means to us and I think diet -- and I think that's I've been so difficult to lock it down. It is a challenge but there is also I think from a social standpoint
, this is an ongoing thing. We are not going to get to a stage where we are just going to say we haven't figured out. We are done. It is a moving target and its ongoing and we are constantly going to be reshaping our privacy, policies and rules so I think to your point around the weblogs which is what, where we get that data from around that what type of browser people are using and operating systems it really is to understand how we can best serve our user community. Understanding what technology they are using so we can adapt our server to protect the technology of our user and it's the same question that the industry has and that really is at the heart of the argument in United States. I should

not say argument but it's the two sides of the discussion is happening on a large scale and it's the industry who is pushing the idea that we need a certain amount of data to best support our community of users but at the same time there is a need to recognize and appreciate privacy and where that balance lives, I don't really know.
>> There was some discussion of the chat about what do you do if a user calls over the phone and wants to know when their books are due and there is some suggestions on how to handle that as far as asking for their library card number to verify that or not giving titles of the items. Anything to add to that?
>> I see a comment from Kathy Hill. Administrations who ask for statistics who are using -- to justify our existence, I think that's something that all of us face and also information that we need to justify which databases we are going to continue and how they're being used and I think that if you get asked for something like okay, if our administration were to ask us for a list of students who use a particular item, our answer would be a resounding you don't need that. We can tell you how many people used the item and we actually are owning a discussion about how we're going to go forward in the future handling those. And I see we are out of time and I'm going to fill out a question out there to all of you. Is this an issue that you think in the depository libraries and with GPO we should continue exploring innocence of determining and setting up a policy or ideas for best practices for the libraries.
>> I'm going to make one -- Erickson said I was reviewing the statement FOIA notwithstanding a librarian is barred by law from being released to anyone because of privacy restrictions. I felt it was not that simple anymore. I agree. It really seems like an overly broad and out of date statement. A lot of good comments and I guess we're out of time.
>> If you have additional comments, keep them coming in the chat box. We are recording all the chat and participants as well as the Council and GPO staff will have access to that. Join us back here at 2:15 PM for the next session of digital only depositories. >>
[Event is on break and will resume at 2:15 p.m. ET]