

>> Kathryn Ratte: Okay, I think we'll go ahead and get started. This is the information brokers panel. Thank you to everyone who stuck around with us today. My name is Katie Ratte and my co-moderator is Loretta Garrison. We're both with the division of privacy and identity protection here at the FTC. And today, we've been discussing the collection and use of information in various contexts. As well as the extent to which consumers are aware of those business practices. And one area where we don't think consumers really understand what's going with their data is the aggregation of consumer data for marketing uses. Earlier, when we were discussing the retail loyalty card chart, Richard Smith talked about the data of Pen Vendor, where you can get additional demographic data for a marketing profile. And that's just one example of how these marketing profiles are enriched in ways that consumers may not understand. There are also data products being sold directly to consumers that are being put to secondary uses in some cases that consumers may not anticipate or like. So the term "information broker" is pretty broad, and it covers a lot of ground, so I want to define, for the purposes of this panel, what we'd like to cover. This panel will deal with unregulated uses of consumer information. And by that we mean those that fall outside of the fair credit reporting act. We plan to talk about the sale of consumer information to businesses for marketing purposes. We'll also call this the "b to b" context. And we plan to explore the business to consumer, or "b to c" context, as well. And for what purposes some of these direct to consumer products are being used and what secondary uses might they be put to. During the previous panel, we also heard a lot about the online collection of data. And here, we plan to look at some of the offline practices in the information broker business, as well as how some of these new online sources are being used to enrich databases created from offline sources. So, with that, I'd like introduce the panelists. First, to my immediate left, we have Jim Adler from Intelius, Jennifer Barrett from Acxiom, Pam Dixon from the World Privacy Forum, Rick Erwin from Experian Marketing Information Services and we hope, very shortly by phone, to have Chris Hoofnagle, from the Berkeley Center for Law and Technology. Chris was unable to be with us in person today. But we hope to have his virtual participation very shortly. Just a quick reminder to the panelists. Please raise your table tent if you have a comment. Although I'll be directing a lot of the questions, in the first instance, to a specific panelist, I encourage a lot of interactive dialogue, so please jump in if you have something to say. Also, if you have a question from the audience, please write it on a question card and hand it to one of the staff circulating. They have extra cards for if you need them. And for those of you listening in on the web cast, you can e-mail your

questions to privacyroundtable@ftc.gov. So, I thought we'd start it off with a pretty easy question. And that's, how to define sensitive information. I'm just kidding. That's not an easy question at all. So, I'd like it start off by asking the data brokers that we have here, what types of information you collect, whether it includes sensitive information, and how you go about defining sensitive information. So, Jennifer, let's start with you.

>> Jennifer Barrett: All right. Let me start with what types of data we collect, because I think that kind of sets the stage. Our data collection practices fall into three main categories. We do use information from public records and other publicly available sources. We use information collected from surveys that the consumer fills out directly themselves, either for us or for other parties that we acquire that data from. And we use information from companies that are consumer facing. And have consumers as customers, and have given notice that the data will be shared by a third party. Our definition of sensitive information actually falls into two categories. We classify all the information that we have at Acxiom, and any of our data products, into three classes. The first is sensitive, the second is restricted, and the third is nonsensitive. Our definition of sensitive information, in this context, is information that typically contributes to the consumer being at risk of identity theft. Restricted information is information that has a sensitivity to the consumer, but probably doesn't put them in quite as much real financial or other type of risk, like a cell phone number, or like an unlisted telephone number, or in combination certain kinds of data that might -- the consumer might be concerned about. So, we have special rules around how we treat sensitive information. Obviously, it's a higher standard of protection. We don't sell to near as many people. In some instances, we screen the client that is acquiring the data to a much higher degree from a security or otherwise standpoint, as well as restricted information, has a set of rules around it. And of course, then, for even the nonsensitive information, we enter into a contract with all our clients, make sure they have a legitimate purpose for it. And depending on whether it's used for marketing or for risk management, there's a set of conditions around what the client can and can't do with the data within their own enterprise.

>> Kathryn Ratte: Jennifer, could I just follow up to that and ask you to give us some examples of categories of sensitive information? You said it was things that put the consumer at risk of identity theft, but that could be pretty broad-range.

>> Jennifer Barrett: Well, any kind of detailed financial information, account information, identifying information, like a social security number or a driver's license number would fall in that category, or a full date of birth, that type of thing, mother's maiden name, that type of thing.

>> Kathryn Ratte: Where would something like health information, or ailment information fall?

>> Jennifer Barrett: If it's protected health information under HIPAA, it obviously falls under the sensitive classification. If it's voluntary information on a survey, typically about ailment information, we would consider that restricted.

>> Kathryn Ratte: We'll come back to the survey issue in just a little a while. Rick, would you like to add to that?

>> Rick Erwin: Much of what Jennifer described is also true for Acxiom. Both of our companies are extremely rigorous in the way in which we collect and care for information. One point I'd like to make, just to back up to the definition of the panelists here, as information broker, I think I can probably speak for Jennifer when I say, our clients don't think of us as information brokers. Because, in our industry, in the marketing industry, brokers are usually entities that never take possession of the information that they are providing to their clients. And nothing could be further from the truth, in the case of either Experian or Acxiom. In Experian's case, we not only rigorously vet every single data source that we have, but we rigorously manage every bit of data that comes through our doors. So, having said that, I'll just say, the data that we collect really falls into three categories. Public data, public record data, which is things like telephone white pages and Census Bureau data, it's self reported survey information, which is where a consumer has been presented with the request to participate in a market research survey, for the express purpose of using their information for marketing. And then the third category of information is permissioned marketing data, and that falls into the category of data that has been collected with the express permission, with proper notice and choice from the consumer, and that could include the kind of information you'd find provided by a retailer.

>> Kathryn Ratte: Okay, and we definitely want to come back to a discussion of exactly how those permissions function, but maybe, Jim, could you tell us a little bit about your categories of information, and what you consider sensitive in your data products?

>> Jim Adler: Sure. For those that don't know, Intelius, we are an online information retailer. We provide search services about people, businesses and assets to consumers and enterprises. We are really a retailer. We obtain a lot of information and we package it up for individual consumption, to consumers, typically. And similar to Rick and Jennifer, how they described the information, it's similar. We obtain data from the industry, public records data, which are birth and death certificates, business records, property title kind of information, also publicly available information, information that's on the web, business information. And then commercial records, what's commercially available. Lists, phone connect/disconnect information, also business profile data comes through commercial sources, as well.

>> Kathryn Ratte: Okay. Sounds like we still haven't gotten Chris to join us. Pam, did you want to talk a little bit about how these definitions of sensitive information function, and what you think might need to change in this space?

>> Pam Dixon: Sure, I think, first off, I think this is an enormously challenging area. The definition of sensitive information is something that we're wrestling with in the state of California, just at state-level, trying to determine what that definition would look like for health care standards, for health information exchange. And let me tell you, it is not pretty, it's not fun. So, I think that these are honest answers. I think that I would offer a couple thoughts. I think Jennifer's idea of information that puts an individual at risk for identity theft is actually not a concept that is frequently seen as the definition of sensitive information. I think it's a good category to add. And I think it's a positive step forward. I do think that there are standards in the EU for the definition of what constitutes sensitive information, and I think that those are important to take a look at, because those standards were arrived at by a thoughtful process and they're robust. I think that the OACD has done a lot of work in this area. And again, it's been a multi-stakeholder process, and those are robust. So, just without reinventing the wheel and going through a whole book of information, I just want to focus on one area, which would be health care information. One of the

great concerns we have, it was brought up earlier in the day when, for example, the med -- the health list was discussed, in terms of those ailments being published, I think that all of us in this room would find and agree that it's fairly repugnant to sell people's mental health ailments on a marketing list and say, "hey, look, these people are easy targets." That's just really, I think, ugly. And I think we can all agree with that. But the way that this information was released was not from a doctor's office. It was because the consumer, themselves, agreed to release it. Therefore, pulling it out from under HIPAA. So, you have the same information that would be held under HIPAA, the identical information, then, with the consumers' own consent, is released. So, when is this protected information? Is it protected just because it's held by a doctor? Or is it protected because there's a reason that it should be protected? And I think that's really the core of what we need to look at. Do we want this information protected, or just the context the information is held in? So, I would argue that we should protect the information, and there should be standards.

>> Kathryn Ratte: And defining those standards, not easy.

>> Pam Dixon: Not fun but I do think it does need a rigorous consensus process that has friction and tension and teeth.

>> Kathryn Ratte: Rick you had something to add.

>> Rick Erwin: I couldn't agree more that a thorough discussion of these things is always a great idea. I failed to answer you on the notion of what Experian considers sensitive data among its marketing data assets. We would consider children's data, data on older Americans, health care data including ailment data, account number data and financial information all to be sensitive data. However, we only collect and provide to the markets the first three. That is to say children's data, data on older Americans, and self-reported ailment data. And we have about three decades of experience with those types of data that I just described being safely used for marketing purposes. And it's not an accident, it's not because there was no regulation and no industrial self-regulation, it's because we've maintained a system where self regulation works and where the industry continually does things like this at this forum and establishes the right balance between the interests of consumers and marketers. For our company when we sell what I just defined as sensitive

information, we not only put every client through a rather detailed credentialing process, we make sure we see the actual advertising piece that they will be using, whether it's a mail piece or a script or whatever. We require that the contract not only require them to sign on to adherence to law and industry self-regulation, but also our own experience on global information values. We randomly seed all of these data files all of these databases with real addresses, with fake names that we can monitor to make sure that they're no in fact, doing something with the data that they didn't -- that they did not warrant that they would be. So the point is that's not an accident. That's because companies like Acxiom and Experian are extremely responsible and in my experience the DMA has represented an industry where that method of self regulation works and it's been working for 30 years. And I haven't heard a lot of examples of where we can point to deep consumer harm because they received the wrong advertising as a result. And I think that's -- we can't overstate that point.

>> Kathryn Ratte: Jim, did you want to add something to that?

>> Jim Adler: Just living down stream from the Acxiom experience, I want to thank you for that, since we are consumer facing. And from our perspective, things falls into three buckets. Clearly the buckets that are clearly sensitive or should be restricted, things like data about children, medical history, telephone conversations. The other side of the spectrum are things clearly okay. Data that people put out on the web, linked in profiles come to mind. Clearly okay to obtain that information. And then we're discussing in forums like this everything in between. And as Pam said it's difficult and transparency and clear debate and discussion are vital to have bright lines around what is okay and what's not okay.

>> Kathryn Ratte: Since we got on the topic of the Med Net list, I wanted to get down into a little bit more detail about how the permissions function when consumers give that you information. How do you ensure that the consent that a consumer is giving to disclose a mental health condition is the type of -- I think Leslie Harris called it serious robust consent that we would want to look for. Put another way, how can we be sure that the consumer actually knows that by filling out this survey, they're consenting to the use of that information for later marketing purposes? Rick?

>> Rick Erwin: I'll tell you what our standard is. Our standard is there is a massive sign at the top of that, if it's an internet survey at the top of that page that very clearly says we are interested in collecting marketing type information, market research information, and we would like your opinion. And it goes on to very clearly spell out from anyone whose data that we would buy to resell for this purpose, it goes on to restate that any data that they provide can be used for marketing purposes with other marketers and advertisers. And gives the respondent or potential respondent multiple opportunities to leave the process without that information being used if they don't choose for it to be used. It's really quite simple and quite clear. In the case of our sourcing standards. I think Pam would like to respond to that.

>> Pam Dixon: Thank you. A couple things. One of the problems that I think has been highlighted today is the role of consent in privacy and the role-- kind of a sub topic of that, opt in, opt out. I think that we need to really look at consent very carefully. Again, we should be informed by consent in the health care sector and what that has become and some of the problems that it's posed to consumer privacy. I think a couple of things. First, in terms of consent, one of the questions I've always had is are the consumers being told, for example, that they're going to be put on a list of people with mental health ailments, are they told their information will be sold for a period of time that does not have necessarily have an ending point in sight. Are they told that they will not have the opportunity to revoke consent at any point. So I think that unless a consumer is given, for example, the delineation of the boxes that they'll be put in and sold in, I don't know that that is sufficient concept. Additionally, I think that there are other issues in terms of mediating consent on line which are well-known issues that the federal trade commission has looked at and GLB and FACTA and fair credit reporting act already. I think it's difficult. So I would say taking the most lenient view of a consent process, in trying to give everyone the benefit of the doubt, let's say that consent is possible for this kind of data online, let's just assume that and go from there, if consent is possible online for sensitive health data, for example, I think the bear minimum would be that a consumer would have the right to know what list they're going on for how long and would have the right to revoke their consent.

>> Jennifer Barrett: I'll be happy to comment. First of all, we only have about eight what I would call ailment categories. Mental health is not one of them. They're very general categories in the

nature of allergies, diabetes, things that a large percentage of the population has and large percentage of the population might be interested in information about because the purpose of this is to get them marketing information about products and services that they may or not have been aware of. But I think Pam makes a very good point and that is consent is important and we do the same sorts of things that Experian does in terms of screening sources, but choice along the line also is. Because if the consumer felt comfortable about it at the time and then maybe their allergies go away, and they're tired of getting marketing material, they should certainly have the right to do this. This is the DMA standard to opt out from marketing and we allow consumers to come to Acxiom and either opt out all together from all of our marketing products or to opt out selectively from some of the different ones if they just want get off of online targeted advertising they could do that. If they want to get out of the telephone directory we produce, and sell the mini web site for white page and yellow page searches they can get out of just that. Or they can get out of absolutely everything.

>> Kathryn Ratte: We've been joined now by Chris Hoofnagle by phone, so I wanted to give him an opportunity to comment. Chris?

>> Kathryn Ratte: Okay, our phone hookup may not be working so well. Until we make contact with Chris, we'll move on to another topic. Jennifer, could you outline for us what kind of screening you do of your data sources -- oh, here he is. Go ahead.

>> Chris Hoofnagle: Can you hear me?

>> Kathryn Ratte: Yes. Speak a little louder, please.

>> Chris Hoofnagle: Okay, but can you hear me?

>> Kathryn Ratte. I don't think it's working. He can't hear us. There's a delay. He should turn off the web.

>> Chris Hoofnagle: Hello?

>> Kathryn Ratte: Okay. I'll ask a question that we got from the audience until we figure out this issue. Could someone comment on what percentage of the data broker industry is represented by the unregulated products that we're discussing hearing today as opposed to FCRA covered products? I don't know who wants to field that one. Maybe--

>> Jennifer Barrett: We'll, I'll start. We have both products that fall under the FCRA regulation employment screening, background screening for employment, as well as tenants, and we have what I think historically is called unregulated products, which would fall under the marketing arena. To some degree I object to the term unregulated and I think my product people back at the office would argue that point vehemently. When I walk in with a whole list of things that they're supposed to do and follow relative to those products, some of them may be legally regulated, for instance there are certain public records that are prohibited by state law from being used for marketing purposes. So obviously we have to follow those regulations. There are also a variety of other contractual obligations that come with the data since we're not an originator of the data. As your wonderful chart on the wall so beautifully depicts. And so we have lots and lots of specific rules and prohibitions on what we can and can't do with the data. And then layer on top of that the fact that the marketing association has a whole set of ethical practices relative to both collection and the use and the sale of data. We don't feel very unregulated even in what most people think of as unregulated products.

>> Kathryn Ratte: Well then I guess the question then is, are there segments of the market that are truly unregulated? Because it's true that Acxiom has the standards that you've been talking about, you adhere to the DMA guidelines but part of the conversation we need to have here is whether there are actually actors out there who aren't adhering to these guidelines, who are operating totally outside of regulation. I think Pam has a comment on that.

>> Pam Dixon: Yeah, it's a challenging question because there's too much that we don't know. I would love to see a list of all folks who are doing -- well, we don't even have a list of folks who fall under the fair credit reporting act; we don't have a list of the specialty databases under the FCRA. So I don't see how we can really get our hands around what this universe looks like other than to give you some very broad ideas, so here's the ideas, and I apologize for not being more specific but

if you look at customer relationship management databases. This is an extraordinary source of unregulated data on consumers. Another, I think area is transactional databases and data co-ops, purchase history. So, for example, you activate a credit card and it's not your credit card company that's doing this, they're regulated, it's the folks doing the activation, you know the third party. They're unregulated. So I really think that you're looking at a universe where you have some very large entities such as Acxiom, Choice Point, actually a lot of folks at this table who do have regulated products, credit bureau things that have permissible purposes or nonpermissible purpose under the fair credit reporting act, but when you start talking about for example badcustomers.com, you know a list of charges that have been disputed, folks like the work number that compile salary information, there are just -- I think there's a large significant universe of unregulated database. But the exact size? I have no idea.

>> Kathryn Ratte: I think we're going to try again to make contact with Chris [laughter]. We'll see if it works this time. Chris, do you have any comment on the unregulated portion of the market?

>> Male Speaker: Give him a second, give him a second. if he's watching on the web, he should turn the web off. Like on a radio show, they say he should turn off the radio show.

>> Loretta Garrison: How long of a delay is it?

>> Male Speaker: Well ,he's watching on the web, he should just turn the web off. It's like calling into a radio show, you know they always say turn off the radio show.

>> Loretta Garrison: We understand he's listening to this via the web cast, not over the phone, so there's a delay. Sorry, he can't hear us.

>> Male Speaker: He should turn off the web cast.

>> Female Speaker: He's not getting the feed any other way.

>> Male Speaker: Oh, he's not? He can't hear us.

>> Chris Jay Hoofnagle: My comment seems to be about a minute delayed.

>> Male Speaker: True. That he is right. [laughter]

>> Kathryn Ratte: Did he have anything else? Okay we'll, we will plow on. I wanted to spend a few minutes talking about what new data points online sources are bringing to your existing databases.

>> Chris Jay Hoofnagle: Because I can't hear, sorry I-- but I can't hear what anyone is actually saying, it's upped over the webcast . So I don't have two way audio.

>> Kathryn Ratte: Okay, we'll keep going, okay. I wanted to spend a few minutes talking about new data points. The previous panel talked a lot about online sources for data collection. We've also heard about new types of information collection such as through social networking sites. And even the smart grid, you know the granular information that may be available on consumers' energy consumption and the possibility that that might be used for marketing. So I was hoping that you could comment on you know not necessarily on whether you're using those new data points now, although that would be interesting, but what rules would apply to that sort of data as you merge it into your existing databases. Rick, did you want to start?

>> Rick Erwin: Yeah, it's very simple. We apply the exact same rules that have worked well for 30 or 40 years in the offline world because those rules are based on principles of balance, accuracy, security, integrity and communication with the consumer. So you know principles endure things like shifts in media channel and that's what we found. So whereas 20 years ago we would have collected data from people self-reported from paper surveys that they would fill out on whether or not they like to golf or whether they had dogs or whatever it might have been, now all of that data for us is collected from the internet but it's done using the exact same collection principles as would have been done before. And as it relates to publicly available information from social media sites, I can tell you that we periodically evaluate that and thus far have not found those sources to square with our own information values so we don't acquire those sources of data.

>> Kathryn Ratte: And which information values are at stake here? I mean is it a matter of data integrity or is this something to do with your-- the privacy interests?

>> Rick Erwin: It's almost always a combination of all of them. And certainly in this case in this example I'm giving you that's very much the case.

>> Kathryn Ratte: Pam?

>> Pam Dixaon: Jim.

>> Kathryn Ratte: Oh Jim, go ahead.

>> Jim Adler: I just wanted to say that in many respects the data that's out there about social networks is in some sense you know flattening the world a little bit. And what we've sort of accepted for the last 100 years have lived in and grown to expect the anonymity of population density and what the web is really bringing it is a community that's new. And a lot of that data is new. And we bring a lot of that data to consumers. And so we see a lot and I hear a lot of, well, you know I want to know everything about you, but I don't want you to know anything about me. You know, and we see a lot -- you know and we're struggling with how you square those two. We have a lot of people show up at our site that want to learn more about people for all kinds of contexts. They may want to date them, they may be-- there may be a long lost relative they're looking for. And there is a plethora of data out there that comprises your digital footprint and we are just at the very early stages of this and it's very important that we look at it from the context of where we've been, but there's also a tremendous value in the connection that it brings.

>> Kathryn Ratte: We have a question from the audience. Oh, Pam, do you want to add?

>> Pam Dixon: Yeah, Please. Thank you. I think one thing I'd like to just point out very very quickly, actually two quick things. One is there's been a lot of discussion of self-reported data, but I think it's very important to understand that consumer choice is fatally undermined when you start

talking about data collection from core service provisions. So, for example, if you are going to be in the Tennessee area and you are under the Tennessee valley authority smart grid, which is going online right now, your electric data and the data of the smart appliances with their unique IDs and all that good stuff that you're using in the smart grid application is going to be collected and massaged and they have grand plans for the data. They've already discussed this. And you know, is there something wrong with that? Who knows. Smart grid is very new. We need standards. NIST is looking at this as most people in this room know. We signed on to Commets with the electronic privacy information center with a lot of detail about this, but the bottom line is that that's not self-reported data. That's a consumer who is just trying to get electricity. A similar situation is with Cox digital telephone. If you sign up for that service, your data will be analyzed for your calling patterns, who you're calling and what kind of turnover you can be expected to have. The consumer choice there is to not have digital phone. And I don't think that's a great choice. So I think we've got to be really careful about making a distinction about especially core service provision, and whether or not there is consumer choice. But the second-- and I'll be very brief. The second point is to look at harm. There's a front page story in the New York Times about an elderly vet who signed up for one of these surveys and got his name on the list and his name was sold over and over and over to list brokers as a kind of a as a soft target and he lost his entire life savings. So I would say that in general self regulation is not effective for 100% of all actors in the universe and we've got to avoid consumer harm. And I think avoiding consumers harms means rules that apply to all.

>> Kathryn Ratte: Okay, Jennifer has had her card up for a while and then I have a couple more questions before we get out of the data collection which is really the first of our topics. So we'll need to speed it up here.

>> Jennifer Barrett: I'll try to be quick, but I it is a good point relative to there is a lot of new types of data like the grid data, that is coming on the market. And I think it's imperative that industry take a look at that data and develop some self regulation even if it ultimately it becomes formerly legislated or regulated requirement. We're very active in the mobile area relative to the new location data, and what does that mean? How should it be used? What kind of controls should the consumers have? And I think that you know social network data and other places where we have

new types of information that we've not seen before. I want to make one though brief comment because there's been a lot of talk about data collection and kind of leaves the impression that once you collect data it kind of then can be used for anything. And so we get into this whole debate about secondary uses. And I think we run and manage our entire business in two very separate segments, one relative to marketing and it can apply standards like the DMA has relative to both collection and the use of that information and opt out and so on, but the other side of our business which not everyone has is relative to risk. And part of that is the SCRA regulated part, but part of it's not. It's identity matchment, it's verifying someone's credentials when they sign up at a website or enter in to a contract with someone and they want to verify that this is a legitimate person. It's know your customer under GLBA kinds of rules. And, and what people want is very different in those two sectors. In the marketing area, and I often see well we want all this granular data and we're worried about the secondary use of it, but the reality is if a marketer doesn't have enough data to make a profit on the cost of developing an approach, creative, copy, production of it, testing of the ad, and then a rollout which requires tens of thousands if not millions of people into a particular category, they're not going to use it for marketing because they're not going to spend the money to develop a campaign, that loses them money. On the risk side, we have a different equation because when we're talking about maybe watch lists or other kinds of data, having someone on that side of the equation can be very few number of people-- it can be very valuable. And we tend to lump both of those all together and want to treat them or want to establish rules as if it was one big pot. And I think we run the risk of not ever getting to the right answer for each sector.

>> Kathryn Ratte: I think that's an important point. I want to get a question from actually from someone watching on the web cast. I believe one of the panelists indicated that they use information found on the web as a source. How do they ensure that this information was legitimately acquired? I think that might have been to you, rick.

>> Rick Erwin: In our case, the way that you phrased it or the question or phrased it, information that we found on the web would not characterize what we're doing. We find that market research surveys that are published on the web seeking people to respond to them, no different than if someone calls your home and says I want to ask you who you plan to vote for or I want to ask you if you're a pet owner, the internet is a very effective and efficient way to collect that information.

And a number of our sources do so and we vet those sources in the manner that I mentioned before, making sure that that the information that we collect from them has always been collected against our -- in consistency with our global information values and the single most important one of those I think for this questioner is the notion that the consumer filled the survey out because it was a market research survey that was going to be used for marketing purposes. That's-- that's our experience.

>> Kathryn Ratte: Okay and Jennifer?

>> Jennifer Barrett: Yeah I just want to add that I think that obviously as all America goes on line, whether we're a consumer or a business, more and more data that used to be collected historically offline is now collected online. Part of our due diligence process, and it's gotten to be quite tedious, but you know we feel it's important to do, we're collecting information from companies that originally collected it online. Now we're not getting it online, but it originated online. And so we actually go out and review the privacy policies at those sites, we reviewed 60,000 privacy policies in the last 12 months. So if anybody wants to know about what privacy policies do or don't say, we have some folks that are extremely knowledgeable about it.

>> Kathryn Ratte: Well I think there are probably a lot of consumers out there that want to know what privacy polices do and don't say. I have question for actually the whole panel, for Jennifer, Rick and Jim. Do you identify for consumers the sources for your information products? So for example, is there any way that you communicate to consumers how your databases are enriched with other kinds of data sources or a consumer comes to you for some reason and wants to know how they acquire the profile, can you point them to any sources? Jim, I'll start with you.

>> Jim Adler: I think that something we're grappling with and consumers clearly want to know. Certain of our agreements prohibit releasing that information and I think as but certainly I think consumers would, A, want to know what type of data. Was it a commercially available public record or web procured information. And, B, ideally if there's any kind of a dispute around the data, the correctness, the accuracy, they'd want to know what is the source of that. And I think we're just at the beginning of providing that level of transparency. We talked a lot about

transparency in earlier panels and I think you're going to see a lot more of that. Consumers are getting much more comfortable with what's out there, but they want to know well then how do I -- is this all of it, what is my digital footprint, how do I gain knowledge of it, and more importantly, if there is an issue, how do I correct it if it's incorrect. How do I maybe even comment on it if it is correct so that when someone does access it, there is a dialogue there. And they could -- right now I think secrecy breeds a lot of mistrust and I think consumers don't know what their footprints is and it nags at them. And I think we are -- as time goes by we're going to be providing more and more information to consumers about their own footprint.

>> Loretta Garrison: Can I ask a follow-up question on that? You said certain of your agreements prohibit releasing the information -- you're a B to C business. What are those circumstances where the information is not made available to the consumer?

>> Jim Adler: So, we, like I said, we either get data from public records or from publicly available information or commercially. And some provisions in our contracts, the source does not want -- there's a non-disclosure provision of that contract. Where they don't want that information being disclosed. I think that that very well may have to be revisited as we move forward as consumers want to know more about their footprint, they want to know where the source is so they can have more visibility into this and be able to take proactive actions if they choose to.

>> Loretta Garrison: And Rick and Jennifer as you also answer that question could you address that issue, as well.

>> Jennifer Barrett: Certainly. We do create and I think I'll speak for Chris even though he's on-- not on or on the phone and can't talk, I think he calls this data providence in terms of knowing upstream where the data came from and we track every single solitary piece of data that we bring into the company and where it come from for lots of reason, not the least of which is being able to know and answer a consumer's question where did you get my data. And I think it is something that the industry needs to be move more aggressively on. We've been doing the where did you get my data for years. And I was pleased about it's either 18 or 24 months ago when the DMA made the requirement a part of their ethical guidelines when a consumer ask a company that receives a

piece of marketing material from them -- or the consumer receives from the company where did you get my name or where did you get the data that this originated this marketing campaign, to refer that to the source. We actually want our clients who we sell data to, to refer consumers to us. Because our clients can't answer that question. And we want to get it answered. And if the consumer has an issue or a problem, we want to get to the bottom of that problem. So our consumer care group fields lots of calls relative to where did you get my data and we're happy to deal with those, inform them of those sources and tell them in case of said public record or other sources exactly how to get in touch if they want to move further upstream.

>> Kathryn Ratte: Rick, did you have anything to add there?

>> Rick Erwin: Only that in our experience, the consumer, we have a similar experience consumer services center that takes inbound calls with questions like this, but in most cases, what the consumer wants to know is not the company from which we bought it or the governmental agency in the case of public record data, but, rather, the category. So typically our answer of it was either a public record source from the White Pages or from the census or whatever or it was from a survey that you filled out last November, or it came from a trusted company that you do business with and gave permission to use your information in I would say 95% plus percent of the cases, that's sufficient and we quickly follow it up with a proactive question of do you want to be taken off of our list and if they choose to do that, then for conservatism sake we don't simply remove them from that one source or database, we remove them and their entire household from all of our databases permanently. Until they ask to be rein-stated. Which they sometimes do.

>>Loretta Garrison: On that last point, do you actually identify a particular company or do you just say it's a trusted company --

>> Rick Erwin: No as I say, we identify the category of data that it was from and in every case that I've ever seen, that satisfies the consumer because in our experience, they're typically not trying to track down an individual company, they're simply trying to understand a little bit more about how this data is used to target advertising to them. They're quite satisfied when they find out what type

of data it is. Either at that point they're satisfied or once they have chosen to opt out of our database, then they're satisfied.

>> Kathryn Ratte: I think Pam has a comment before we get more into the issues of opt outs.

>> Pam Dixon: Thank you. Our experience, just to provide a little bit of consumer perspective, our experience is quite different. We spend a lot of time on the phone helping people who are having reputational harm issues. So, for example, people who have been blackballed because some complete crazed person has posted ridiculous things about them on the net. Usually an ex-boyfriend or girlfriend or husband or wife, something like that. These cases are very tough to tackle. And additionally victims of various forms of identity theft come to us with very similar questions, people who have bad reputations in some of these you know kind of murky corporate databases where they don't have access to, they want the company names because they want to clean up their files. And I cannot express to you adequately how frustrated consumers are by the lack of ability to trace down the root of the data and pull it up and get rid of it.

>> Loretta Garrison: Thank you. I'd like to turn to the opt out-- how it's, what you offer, how you offer it. But there's a threshold question which some in the audience have asked and that is how do consumers even know that you exist and how to find you.

>> Jim Alder: I'll start. Can I start with that? Because they can find us pretty easily. There's I think Comscore said you know about 12 million people came to our site monthly. A little higher than that these days. So we're pretty easy to find. We power a lot people search around the web, and so once they find us then what can they can they do once they get there. And we recognize that this is a really important developing area where we need to provide -- we're going to get into opt outs in a minute, but once they find us, then the question is what can they do to proactively take control of their footprint. I think it is what is coming for the industry and we need to step up and provide that, because consumers clearly are frustrated and when they do realize that they have a digital footprint, yes, it matters and for reputation reasons and for everything that binds our society trust and success in our society depends on your reputation. That's clearly being driven more and

more online and we need to provide folks the ability to control their digital footprint. The first step of that is to have transparency into it.

>> Jennifer Barrett: Ah yeah, there are a couple of different ways and it somewhat varies by product. For instance, our telephone directory that we license to a lot of large companies that provide white page online services says power by Acxiom and you click on that and that takes you to us and our opt out and so on and so forth. For-- we are actually moving a little bit more directly into the area of direct to consumer. And we now offer the consumer to get the same background screens that an employer or landlord might get if they so choose to. And actually in today's employment market, a lot of people want to have that in hand when they go apply for a job. In the marketing arena, we encourage all of our clients as I said earlier to refer the consumer to us if there's ever any question about where the data came from and we are referenced and linked to by most of the privacy websites so that the consumer has the opportunity to get to us via that vehicle as well.

>> Loretta Garrison: Do you-- can you estimate about how many people opt out say on an annual basis?

>> Jennifer Barrett: Varies a little bit from year to year, but it's in the 20,000 to 30,000. We've dealt over the last ten years with about a half a million consumers either for opt out or accessing correction purposes.

>> Kathryn Ratte: rick?

>> Rick Erwin: Yeah, I'll just add-- Jennifer summed it up nicely. Our experience is about 7200 consumers a year choose to opt out. But they can find the link to Experian to do so either on any of the Experian marketing websites, the phone numbers we publish, the DMA choice service which is readily accessible. As Jennifer pointed out, the websites of every privacy agency I've seen have links to this, as well as nearly all if not all state's attorney-- attorney's general websites. And on Friday just out of curiosity for myself because it's been a while since I did this, I goggled marketing opt out and direct mail opt out and in the first two pages there are numerous, numerous links. So as

the-- as the American consumer goes online as most of them have in one way shape or form, there are many ways for them to opt out.

>> Loretta Garrison: Let me just do one follow up. I wanted to ask a little of each of you, what of the data bases that you maintain can a consumer opt out of and what's the method, the process by which they can opt out, and what exactly are they opting out of? I know it's a three part question, which is the worst thing you can do, but, rick, why don't we start with you.

>> Rick Erwin: So, first of all, they can opt out with us in several ways. They can do it over the web, they can call us on the phone number that they'll find anywhere that we have a link for this, and when they do that, if they opt out, they opt out of every marketing database on which we have their name.

>> Loretta Garrison: Is it only for marketing? Or is there other data bases that they can opt out of?

>> Rick Erwin: Well we have a risk side to the business as well. But just speaking about marketing data for a moment, they can opt-- they can call our marketing opt out sights because the rules governing these different data bases are different. And they can-- say I want to be taken off of these databases and their individual name as well as their entire household contact record will be taken off all of our marketing data bases forever unless they call to be specifically reinstated. Then the other principal way is that we would receive their opt out as part of a suppression list that comes to us. For example, the DMA's mail-- mail preference service or DMA choice provides a suppression list of opt outs that they've captured. And we regularly, monthly, process those suppressions through our database to ensure that names take that came through that way are suppressed. And then further the state do not call and federal do not call lists, the same-- the same type of process flow applies.

>> Loretta Garrison: Okay, the DMA list is a five year period, correct, on the mail suppression. So do you honor five years under the DMA when you get the list from them or do you in fact make it permanent as your own?

>> Rick Erwin: We would honor the DMA's five year rule because that was the way in which the information was collected. And the-- if you will, the arrangement that existed between the consumer and the DMA at the time.

>> Loretta Garrison: Okay, and the opt out is tied to the consumer's name or to something else?

>> Rick Erwin: to the house hold in which they live in our case.

>> Loretta Garrison: Which would mean household would be an address?

>> Rick Erwin: yes.

>> Loretta Garrison: So if they move, what would happen?

>> Rick Erwin: It would follow them because in the manner in which we compile the information, we would notice where they've moved to and if they had been an opt out, we would not reactivate them as a marketable consumer just because they took up residence in a new location.

>> Loretta Garrison: Thank you, Jennifer?

>> Jennifer Barrett: For the risk side of our house, we do not allow opt out. Opting out of-- identity verification applications, lists of terrorists and others is just not appropriate, so. But we do offer access and correction because we want to make sure the information is right. So, but you can't get off those lists just like you can't get out of your credit report or credit file. On the marketing side of the house, we offer both broad opt out of everything we have in the marketing arena or granually as I said earlier some of the individual products and services. It is a forever opt out and we do except opt outs just like Experian does from the DMA and others and we honor their time frame, whatever it is. We receive; also, FDC state do not call opt outs and so on. Our opt out is at an individual level, and-- but in some instances the data is aggregated by household and when it's only sold by household. If it's-- if one individual opts out, it opts out the whole household. However, in

other instances where we're selling in at the individual level, a husband can opt out and a wife would not. And what was-- I'm sorry, what was the third question?

>> Loretta Garrison: The method, and I just wanted to clarify the opt out is tied to the address?

>> Jennifer Barrett: In our instance, it's tied to the person.

>> Loretta Garrison: To the person.

>> Jennifer Barret: Right.

>> Loretta Garrison: So if the person moves, the opt out --

>> Jennifer Barrett: It may follow them if we know if they've moved. It may not. And we clearly tell them in the process that when they opt out, originally that if they move, we recommend they come back and re-opt out just to be certain.

>> Loretta Garrison: And then the process by which they can opt out?

>> Jennifer Barrett: Oh, the process is-- you can e-mail us, you can call us, or you can go online and download a form. We have a form that we require you to fill out that asks for certain information. We've had a myriad of interesting experiences over the years with opt out. Maybe the-- one of the most interesting ones, an employer who sent us a list of 375 employees, including their social security numbers, requesting we opt them all out on their behalf. Which we promptly sent back and advised that that was not going to happen. But-- we do ask the consumer to sign and send in the form for the process. In that process, by the way, I'll mention we send them a booklet which people can go online at acxiom.com and take a look at it's intended for consumers, it talks about how their information is used how we use it and others, not just Acxiom, how it's collected both on and offline and you know what other choices they have to opt out. So we feel like educating the consumer and having an informed choice about opt out as opposed to just saying oh I think somebody said I should get out of Acxiom, so let me go opt out from Acxiom, is important.

>> Loretta Garrison: Jim.

>> Jim Adler: So on our site, there's sort of two flavors, one is the public records side-- and it's by, again individual, we don't have marketing lists, so that's really not appropriate, but if you want to opt out yourself, we require proof of identity so we get the right, the right person to opt out. That could be by a fax, just a faxed proof of identity. It's forever. There's also on some of our sites just white pages data that you can typically opt out online during-- from some of our partners that publish our white pages data. There's some-- like Jennifer said, there's some information you can't opt out of. You can't opt out of criminal records, although we do respond to expungements requests. Did I hit all of your points?

>> Loretta Garrison: Yes, Pam, you had some comments.

>> Pam Dixon: I do. Thank you. I'm going to scroll back a little bit to the audience question about how does a person find all these opt outs. It was said today, let 10,000 flowers bloom. What I always say is well if we've got 10,000 databases blooming, how on earth is the consumer supposed to find out about all of them? It's very challenging. And so I have a proposal for the federal trade commission. Just what you want to hear huh? For some time now, we would-- we have really, really wanted to see two things. One is a registry of entities that are regulated under the fair Credit Reporting Act. Two, a registry of specialty databases that are regulated under the Fair Credit Reporting Act. I think that if the federal trade commission could determine who is regulated under the FCRA, and then create such a list, I think it would help consumers enormously. There is not an industry stomach for doing this. We've asked. There has been no appetite. So I think it's going to be left to the federal trade commission to do that. In terms of unregulated databases, I think that this is, you know when industry talks about self regulation, I would throw down the chalice and say this is your opportunity to create your own list of every database out there and provide a single site for consumers. And there will be challenges, but someone's going to have to do that at some point because the consumer harm here is too great particularly with the bad actors. There are just some incredibly bad actors out there who have never heard of the word opt out and wouldn't even dream of letting a consumer do that. And we've got to be more worried about them than anyone else. But

to get back to your current question to kind of reel that back, there's a couple of issues that we've-- we have traditionally had with opt outs. One is cost. I really do think that opting out for consumers, needs to be free, period. End of sentence. Saba search I know they have two opt outs, one is the slow opt out, that's free by mail. The second is the expedited opt out, that's 20 bucks. I don't know about you, but that just doesn't hit me the right way and I don't think that's entirely fair. I think it's worth discussing. Secondly, the use of opt out information for further developing the database is incredibly problematic. Under the fair credit reporting act and under the annual credit report, this kind of thing has been taken care of by the federal trade commission writing good regulations. We don't have this same regulation in the opt out space. So there are some bad actors out there when they are like we have a fabulous database on you, make sure you're not black listed, opt out here. Here's all the amazing amount of information that we need for your opt out and oh by the way we're going to use that, too. So I think that we need to have some regulation about how opt out works for consumers. In terms of the third point I would make is that if a company is operating primarily or substantially online, an opt out should be available for consumer online, not just by mail. There are some companies out there who the only way you can opt out of their online products is through snail mail. And we actually have an open letter to the FTC about this issue with some companies and I think that that's something that also needs to be addressed. It's a more-- more subtle point, but it's still an important one. Opting out should be easy and I really like the idea of a permanent opt out. Thank you.

>> Kathryn Ratte: Okay, I appreciate that Jim and Jennifer have their cards up, but I think we need to move on to the issue of access and correction, which has come up a few times today. I was hoping that the panelists maybe starting with Jim could talk about what access and correction rights consumers have with respect to their data products.

>> Jim Adler: Right now not much, to be honest. And I think the discussion of opt out is sort of the first stage of that, or at least access is important. I wanted to-- before the panel I wanted to see how many people can run their own reports on our site? It's a number I'd like to get and that question may come up, but you know it's something I want to run down. I think people want to know about their, their own-- their own profile. I think that's, that's really important. They may want to opt it out, they might want to opt out certain pieces of it. They may want to correct some of

it, dispute some of it, comment on some of it as I mentioned. I think that this is a-- an area where we need you know the best minds to come together and discuss it. We just went through a trustee audit and it was tough. And they went through top to bottom and the seal was issued a couple months ago now and the reason I want to get them engaged in the company was that this is the beginning of this dialogue. The seal was not the objective. This is the beginning of a dialogue around how do you appropriately provide access, what should be free, what shouldn't be free, what should be some value-added services that we could add on to this. When you bring groups like this together, they have the purview of many industries it was said this morning that trial and error is one of the best tools. There's a lot of tools in our tool box and trial and error is one of the ones at the top. But when you bring industry leaders together they have the purview of many trials so that we don't make so many errors. And I think that's really important when you're talking about providing consumers really valuable services like how do I get access to my profile, how do I identify who I am in order to have purview to it, and then how do I dispute certain elements of it and ultimately correct them.

>> Kathryn Ratte: and Jim, before we move on from you, I just wanted to ask, going back to the opt out question, under what circumstances could a consumer opt out of your database?

>> Jim Adler: They just have to-- like the last question, all they got to do is-- is fax in proof of identity and it's opted out and it's per individual and it's gone forever and it's free.

>> Kathryn Ratte: Okay, and how long has that been in place?

>> Jim Adler: Well, certainly since I've been there. But you know, the last year-- two or three years probably.

>> Kathryn Ratte: Okay, Jennifer?

>> Jennifer Barrett: Yes, let's take first the risk, and then or the nonmarketing and then the marketing products. We offer full access in correction services after authentication of the consumer's identity for all of our nonrisk products. Get very few requests for accuracy and actually

we pay a lot of attention to those for correction purposes because that says we have something wrong in the data. And if it didn't come to us wrong, then, you know, we want to know about that. So it's a good quality control for us. That offering goes back to the 1990s back when the old IRSG days, where that was part of the self-regulatory initiatives way back then. On our marketing products, we do not offer access or correction we offer the opt out and we offer what we call robust notice which is a description of the kind of data that we probably or might have in the file about you and if you don't want us to use it for marketing purposes, then the correction is essentially a removal or an opt out.

>> Kathryn Ratte: Rick, you're nodding, does it operate the same way at Experian?

>> Rick Erwin: It operates much the same way on the marketing side and I would just go a step further to say access and control for marketing information is neither appropriate nor practical. Jennifer did a good job of saying why it's totally appropriate and practical for credit databases and for fraud databases because if there's inaccurate information in a credit or fraud database, somebody could be denied a loan or employment or something else that they may have a right to. So the information has to be absolutely correct. There's one thing that people could walk away understanding about marketing databases that they may not have understood coming in is that the marketers themselves do in the care about the individual information they're in. They care about segments of the population that will be likely to respond to a marketing offer because they just want to be more successful and more relevant to their clients. The challenge that we have with access and control for marketing databases is there is no one standard of truth that could be established. And unlike in the credit and risk world, it's not as important to a marketer to be that accurate. Most of the marketing information in our databases is presented in estimates or ranges. And that's good enough for marketers so that they're not marketing women's clothing to men or vice versa, things of that nature. And so access and control is just sort of not appropriate in the marketing world but to allow it would open it up to a standard of accuracy that would violate our own values. We couldn't ensure the accuracy of the information when it was-- when it was provided by somebody who couldn't verify it for us.

>> Loretta Garrison: So to follow-up on that point, then if you had really good robust demographic information, would that satisfy the marketers' needs? Because you said a moment ago that it didn't need to be that accurate, but you just need to be able to make the distinctions between say a man and a woman when you're marketing clothing for example.

>> Rick Erwin: Yes. And broad I used an example of a broad category of demographics. The same he would be true of age and estimated income and things of that nature.

>> Kathryn Ratte: Over the past couple of panels we've heard about new tools such as the Google ad preferences manager that allow consumers to go in and tinker with their marketing profiles and in a lot of cases we're hearing that rather than going in and opting themselves out, consumers are in some cases adding to the information and you know, actually giving you more. So do you see a demand for consumers to update their marketing preferences in this context? Wouldn't you want more accurate information if you could get it?

>> Rick Erwin: Well, their preferences and what the information itself is are two very different things. I think when we talk about preferences, certainly we at Experian believe that we're always working towards a better notice and choice and adherence to consumers' preferences. And an example of that is just the way that the DMA has moved from a mail preference service to one that in the future will enable opting out of individual brands' offers. So preference is one thing. And, yes, we broadly support -- we will never stop improving the amount of preference that we make available to consumers about how they're marketed to. We believe that's one of our values.

>> Kathryn Ratte: Pam's had her card up for a while.

>> Pam Dixon: Thank you, thank you very much. I just want to make a couple of statements. I think Jennifer said something that's important that needs to be listened to and that is that the risk databases are different than the marketing databases. I think she's right. And something that we've said for quite some time now is that there's a bit of a risk loophole. If you look at any statute, there's usually an exemption for risk based databases or risk based consumer data to be collected and used. And, you know it's really hard as a public policy to have, you know a position against

this because there's good evidence that some of that data is useful. Here's where the problem is. And I think here is where the fair credit reporting act like right structure or something similar to that or taken from that mold would be very helpful. So, for example, let's say we have -- I call it the risk loophole. Or the anti-fraud loop hole. So we have a risk database. What's your product name?

>> Jennifer Barrett: We have several that-- identity verification product.

>> Pam Dixon: Okay, so let's talk about identity verification. We've got an identity verification database. There's also a company named ID Analytics that does this. These are folks just trying to verify identity for employment and other purposes. Probably law enforcement purposes, as well. I know several health care providers that are using these kind of structures to authenticate doctors and patients. So we can't say no to this. But I think what we can say is this. Okay, we're going let you use this consumer data that's risk data, but we're going to regulate it and here's how we're going to regulate it. We are going to say that the data is going to be subject to governing laws that require permissible purposes, the permissible purpose is anti-fraud. You can't then take the anti-fraud data and use it for marketing purposes or other purposes. And I think that companies like Acxiom would not have any problem with this because they're not doing that. So if you have good actors, I don't think this kind of regulation will be a problem. But we've seen very small companies put up a shingle and I'm talking, you know, like one and two person shops, and saying we're anti-fraud specialists, give us your data and we'll work with it. Yeah, they'll work with it, but no in the ways that the company working with them or the consumers would expect. So I think there can be some, some regulation of risk products that's very beneficial to the entire sector. And I think that's it for now other than I would say that the one push back I would give to you respectfully is that I do think that categorization of data is becoming much more granular and I think we're entering a world where we're micro targeted as opposed to the broader segments of the past. I think that's something we'll see change either now or tomorrow.

>> Kathryn Ratte: Jim, you had your card up.

>> Jim Alder: Jennifer do you want to --

>> Jennifer Barrett: Yeah, I'll be quick. Just to kind of follow up on Pam's comment, we certainly wouldn't object to regulation on the risk side. In fact, we're already regulated because one of the things we do is we as part of the risk products include credit header data which is upstream regulated by the Gram Leach Bliley Act and can only be used for fraud purposes. Now, if you don't include that data in a risk product, then you may not -- you may be outside the scope of that regulation. But I think most of the big providers do because it's a great source of identifying kinds of information that's very current and very accurate.

>> Kathryn Ratte: Jim.

>> Jim Adler: Sure, I just wanted to reel it back to the-- what Alan Davidson talked about on the Google ad preferences. As he said it's still early, but people are not panicked and not opting out, but they feel quite empowered by those kinds of tools. One of the things that we are introducing is a stream line to opt out for vulnerable populations. We recognize that information is powerful, we're working with domestic violence groups, and elected official, law enforcement, to make sure that their opt outs are streamlined and as we get our arms around making those tools usable, we would grow them into a consumer offering, as well. So I think there's a lot of innovation to be done here and it all centers away, hey, what is my profile being able to identify it and then access it and control it and have direct influence on it. And blog what Google is doing, and we're trying to do something similar on our side.

>> Kathryn Ratte: Okay, we have one minute left, so I'll do one more question. And this sort of plays on of a point that Pam just made. But, also, some conversations that we've had with the folks on that panel informally about what they're doing to screen their data suppliers. You know we understand that there are a number of data suppliers who don't meet your standards, and so you won't purchase from them which means there are actors out there that aren't playing by the rules. So I'll pose with the question do you favor increased regulation and this space and if so what elements should the new rules include? And I throw it open to the panelists.

>> Jennifer Barrett: I'll start. I don't know that we need new regulations because what we're doing is screening -- well, legally, what are they collecting the data in a legal matter, but then also what does the privacy policy say, and if they've got a posted privacy policy I view that as something that the FTC could already take action on in terms of understanding are they following that policy appropriately. We also where we encounter a policy that we're not quite comfortable with, we actually try to work with the company to say we think you should fix it this way and it's all shades of sort gray, it's not really clear to they don't even say it or they say this and do that. So there are various aspects that we feel like in certain instances we can work with them and improve the process.

>> Kathryn Ratte: Anyone else? Pam?

>> Pam Dixon: I think self-regulation has brought in the larger companies, but not the smaller companies where so much harm has accrued. That's where you see the really bad actors, just ridiculous cases of harm where consumers call us and their lives are wrecked. I think we'd all like to avoid that. I think the only way to do that at this point is through some kind of model that takes a fair credit reporting act like approach says look, here's permissible purposes, here are nonpermissible purposes, and it will have to be nuanced and I'm not saying it will be easy, but I think it's an approach that would have a very good chance of working. I think the fair credit reporting act has been a very good privacy law. And has been very functional and helpful for consumers and I think that it provides business with reasonable guidelines and I think we can do the same thing here.

>> Kathryn Ratte: Okay, I think our time is up, so in closing I'd like to apologize to Chris Hoofnagel and invite him to submit any thoughts or reactions to the panel discussions through our written comment process and please join me in thanking our excellent panelists. It was a great discussion. [APPLAUSE]