P R O C E E D I N G S

- - - - -

MS. OHLHAUSEN: Good morning and welcome to the Federal Trade Commission's workshop on Information Flows. I'm Maureen Ohlhausen, the Assistant Director for Policy Planning at the FTC. I just have a few administrative details to go over before we get started.

First, I'd just ask if everyone would please be sure that the ringers on your cell phones are turned off. Also, in the unlikely event of an emergency security staff will give us directions.

Just so you know, we're having this workshop transcribed and the transcript will eventually appear on our website, www.ftc.gov, where there will be a link to the workshop's home page.

Also, we will accept written comments for 30 days following the workshop, and the instructions for submitting those comments are on the workshop's home page. Also, I would like to acknowledge that our refreshments were very kindly provided by Experian and Teradata. So thank you all for coming and I'd now like to introduce the Chairman of the FTC, Tim Muris.

COMMISSIONER MURIS: Good morning. On behalf of my fellow commissioners, welcome to the Federal Trade Commission's Information Flows Workshop. We will examine the benefits and costs to consumers and businesses of the collection and use of consumer information.

Our economy generates an enormous amount of data. Most users of this data are honest businesses who have incentives to collect and use information responsibly to serve their customers better. The information revolution greatly benefits all of us. The average American today enjoys access to credit, financial services and shopping choices that earlier Americans could never have imagined. Today we can pay bills, make travel arrangements and go shopping when and where it is convenient for us.

Ordinary consumers can receive the type of personalized service that used to be available only to an elite few. What I personally find most astonishing is what occurs all over America at auto dealers everyday. If consumers have good credit, they can borrow $10,000 or more from a complete stranger and actually drive away in a new car in an hour or less. I call this the miracle of instant credit. I have been assured that it requires a higher authority than a credit manager to bestow a miracle but I still think it's an astonishing thing.

Despite the benefits of information sharing, it is conven consumers willingly part with personal information every day to facilitate transactions.

For example, few consumers seem worried about the many companies that have to share their information to clear checks or to process ATM transactions. They understand that the information must be collected and shared to complete the transaction. Consumers also provide information to increase their convenience or expand their choices.

What consumers are most concerned about is that their information, once collected, may be misused to harm them or disrupt their daily lives. These kinds of adverse consequences drive consumer concerns about privacy.

The FTC's privacy agenda focuses on stopping the kinds of practices that can harm consumers. For example, many consumers are concerned about physical consequences, especially for their children. The misuse of information can cause economic consequences ranging from the improper denial of credit to loss of a job. In extreme cases misuse of information can lead to identity theft.

The Commission’s focus on stopping misuse of information highlights another issue, the explicit recognition of the trade-offs involved in regulation. Privacy is not, nor ever can be, an absolute right. We are willing to make practical compromises between privacy and other desirable goals like having our briefcase or backpack inspected at the airport or before entering a building or a sports arena.

There are trade-offs in the commercial arena as well where information sharing poses risks but also offers enormous benefits. The advantages of instant credit approval, the lower cost of processing transactions and the convenience of personalized services are all benefits that consumers want and expect.

We must ensure that our approach both protects privacy and preserves the important benefits of our information economy. To spur a rigorous and balanced discussion of these important issues, we have invited to the workshop knowledgeable participants with a range of perspectives. More research needs to be done to provide the information that we as policymakers need to understand fully the role of information practices in our economy.

This workshop will help lay the groundwork for future research in privacy and information practices. The workshop will begin with a roundtable of distinguished executives from a variety of businesses that use consumer information extensively. The participants will discuss how their particular businesses collect and use information, the benefits of this information, how their businesses

19

value of consumer trust.

This roundtable will be followed by remarks from my colleague, Commissioner Oalue o-0sionewindliss-870I g 8Itiue of will also discuss business use of transaction data and other consumer information to identify and target consumers' preferences for marketing and the costs and benefits to consumers of such practices.

After the second case study panel, Commissioner Thomas Leary will address the workshop. We will then have a methodology panel comprised of academics and researchers who will discuss how to evaluate the benefits and costs of collecting and using consumer information. Panelists will present a range of perspectives on the appropriate methodology for evaluating information practices including the appropriate use of benefit-cost analysis.

The workshop will conclude with remarks on the use of information to fight identity theft by Wayne Abernathy, Assistant Secretary for Financial Institutions, Department of the Treasury.

Let me move back over here and we will start our roundtable. Let me introduce our panelists who will each make some brief remarks and then we'll have a discussion.

Charles Morgan is the company leader of Acxiom Corporation. Acxiom provides databases and information management for many of the largest companies in the world. Charles, as we were discussing just a few minutes ago, also was the 2001 Chairman of the Direct Marketing Association and he assured me that he does not share all of DMA's current views about the Federal Trade Commission.

MR. MORGAN: No, that was private, and it's true.

COMMISSIONER MURIS: John Thompson is Chairman of the Board of Directors and Chief Executive Officer of Symantec Corporation. Symantec is a leading provider of Internet security technology including the Norton brand of consumer security products. Last year, President Bush appointed John to the National Infrastructure Advisory Committee.

Pete Kight is the Chairman and Chief Executive Officer of CheckFree Corporation, which he founded in 1981. Today, CheckFree is a major player in the electronic billing and payment industry, and he also, like me, was born in Ohio and went to school in Southern California. Actually, he went to Bakersfield which is in between Southern and Northern California.

MR. KIGHT: Very in between.

COMMISSIONER MURIS: Very in between. There are more people from Oklahoma in Bakersfield than in Oklahoma, but that's another story.

Ken Seiff is the cofounder and Chief Executive Officer of Bluefly Incorporated which sells designer apparel and other products through its Internet retail site, bluefly.com. Prior to Bluefly, Ken was the founder and CEO of Pivot Rules, a leader in golf apparel.

businesses can offer targeted compatibly-priced offers on relevant products and services and access to information has accelerated the accuracy and accelerated the speed at which transactions can be completed.

Chairman Muris talked about getting an auto loan. I would also say that the insurance underwriting process, which literally used to take weeks, is now done in hours. And not only can the underwriting process be done in hours, you can shop for insurance online and do it in a matter of hours.

So the flow of consumer information for appropriate uses, such as the ones that Chairman Muris and I have described, clearly benefit the consumers and clearly benefit businesses.

But I want to be very clear on one point. The inappropriate use of information to defraud and discriminate against consumers should be, and in many cases already is, illegal. And those laws should be strictly enforced.

Acxiom is involved in several distinct uses of consumer information, and each provides a different value to consumers and to the businesses that use that information. And, in my opinion, each requires different polin, Dc,t pro1oe001 revayhosr-4irst,c(15)Tj/TT2 Tf4helps21 manage and keep accurate the information that they have on their customers. The second area is information that helps businesses find and keep customers and also grow those customer relationships over time, and thirdly, information that helps businesses manage the various risks that they face in delivering their products and services like the underwriting process that I just described.

In my comments today I’m going to focus on the first issue, data accuracy. Accurate information is the absolute foundation on which mutually beneficial business consumer relationships are based.

Data errors compromise every aspect of these relationships with varying consequences. For example, an inaccurate address can keep a consumer from receiving an item ordered from a catalog. It may be no big deal, except to that consumer. However, being mistaken for a different consumer with a similar name can result in being denied credit in that auto transaction that Chairman Muris described earlier.

Our experience in working with some of the world's largest, most sophisticated companies show that they typically have between 8 and 13 percent error rate in identifying information that they have on their own customers.

Sometimes the data is captured wrong, the

Acxiom provides is demonstrated by one simple customer example. We did a mailing of three and a half million records. We reduced the return mail by tenfold and the annual result of that was a million dollar savings to that one customer.

So the economic cost of inaccurate consumer data to the U.S. economy, I think, goes well beyond advertising. It results in delayed bills, late payment fees, lost payments, undelivered product recalls. And, of course, the cost to straighten out all these messes has not even ever been calculated as far as I know.

Access to third-party data can help clean up consumer records in other ways as well. It can remove records based on a consumer’s preference not to be contacted.

For example, Acxiom provides a suppression service that helps businesses ensure that they don't contact marketers who are on the do-not-call or do-not-mail list. And this task of identifying people on those lists is a lot more complicated than one might imagine, particularly on mail suppression.

For example, if you've got J. Brown at 135 Oak Street on a targeted mail solicitation list that could be John Brown at 135 Oak Street, apartment 4 or Jane Brown at 135 Oak Street, apartment 42. If we had other information about the person at that address, such as age, it could be used as a tiebreaker so that the correct person is sent mail or not sent mail.

If the person on the solicitation list is 34, and we know that John is 75 and Jane is 34, then we know that the J. Brown on the solicitation list refers to Jane. And since it is Jane on the promotion list to mail, it is her name that should be checked against the do-not-mail list.

Acxiom analyzes our customers' data and one analysis going across 400 million customer records and prospect records that represent a cross-section of our clients' data demonstrated a tremendous opportunity to improve the quality and consistency of that customer data.

We identified 21 million of the 400 million records had undeliverable addresses when we first received the supposedly clean customer data. We also identified 9

w1-lj/Fto1wretss

verification and correction services must be allowed to continue to help businesses manage their data accuracy issue because I believe everybody wins.

Restrictions on data should be focused on how accurate information is used, not on inhibiting businesses' ability to get the data right in the first place.

But I think a disturbing trend in recent years is legislation and regulations that unnecessarily curtail the flow of information available to businesses and information that is exchanged between businesses.

I believe in most all cases the motives have been understandable and even laudable. They want to protect the consumer. But in many cases these laws and regulations were created without a full understanding of the facts. They therefore have had unintended negative consequences by restricting or eliminating flows of information that are beneficial to all.

So when drafting effective privacy legislation regulations, though it is not easy, I think a careful study of all the uses of information should be undertaken before restrictions are imposed to ensure that the desired result will be achieved and also, of course, to avoid these unintended negative consequences.

But anyhow, Chairman Muris, we really appreciate the opportunity to be here and participate in this, and we hope that we have been able to make a contribution. We have, in addition to my comments here, a written submission in which I have given more examples and more information about use of data and data errors.

I want to thank you very much for holding this workshop. I think it's a valuable thing to do to inform this debate on the benefits to both businesses and consumers. So I appreciate very much the opportunity to be here. Thank you.

COMMISSIONER MURIS: Thank you very much, Charles. Next, we have John Thompson.

MR. THOMPSON: Thank you very much. And I, too, appreciate the opportunity to talk about a very important topic, not only to our company but, I think, to consumers around the world.

When I think about the issue at hand, the first word that comes to mind is trust because it is, in fact, imperative that we establish a trust relationship between our consumers and our company. As the leading provider of Internet security technologies for consumers around the world, we have more than 120 million users who depend on us to deliver trusted information to them about the security of their environments.

Hence, our goal is to create a sense of confidence in those consumers not only in our company, but in their ability to work and play in a very connected and wired world. So to that end we take this issue very seriously and we approach it with four fundamental tenets of how we want to manage our relationships in this marketplace.

First, policy; second, process; third,

solutions and vulnerability assessments are critically important to how we manage the technology around the information that we have collected.

And finally, organization. The information that we collect is owned by the marketing organization of our company, and they must guard that with all due care because it can undermine the confidence and trust that our customers have in us and, hence, all activity and requests about information in our database must be coordinated through that one organization.

Now, let me give you a couple of practical examples of why those four tenets are important. First, we are one of the most abused companies in the wired world. Our products are very important to consumers yet some people who have dubious intent have chosen our brand as the target for fraudulent spam campaigns.

As a matter of fact, in 70 percent of the campaigns that we have tracked back there has been some fraud motive, either credit card theft, counterfeit software product or, in fact, identity theft of the individual who is engaged on the other end.

So we work hard to protect the brand and have, in fact, made significant investments in enforcement around this idea of protecting the information that we have so consumers don't assume that we are the source of this

deliver better services to those customers.

So it is important that they know that we are collecting information that is a result of the test that has been run on their machines that they have allowed us to do and, hence, we must protect those results and use them in a way that they consider to be very appropriate for our individual or firm use.

So I can’t stress enough the importance of building a trusted relationship, and I can’t stress enough the requirement to build policies, process, technology and organizational controls around this issue. If that is done I believe we can, in fact, continue to derive real benefits from the use of technology and, candidly, the advances that have occurred in the wired world. Thank you very much.

COMMISSIONER MURIS: Thank you very much, John. Pete?

MR. KIGHT: Well, I can tell you it’s always very good in a panel situation when you are able to say I’m going to agree exactly with the person who just spoke ahead of me. It beats the heck out of the alternative. I’m really going to second almost exactly what John talked about but from a very different technology company perspective.

Now, let me tell you just one minute about what CheckFree does since you probably don't know our name but

It is estimated right now that the 10 million people that we have online and our competitors have about another million only represent the very beginning. As we speak, over the last 18 months Internet banking and specifically receiving bills electronically and paying them electronically, online, is the fastest-growing service on the Internet.

More consumers and more households in the United States are going online to activate the ability to see and pay bills than for any other reason that they're going online. And that’s important to understand when you think about this issue of privacy and what we're doing about ensuring it.

It is estimated that by 2006, more than half of the United States banking households will be banking almost exclusively online. So we're talking about a mainstream issue here when you talk about privacy and the fact that people's financial information is going to be online.

We are much more concerned about privacy and security, which we link directly together, because they are interrelated in our part of the business because that is exactly what our customers demand.

We believe that we are in a business that is zero defect tolerant in terms of errors and zero defect tolerant in terms of privacy and security. We don't have any leeway in that business whatsoever.

I will tell you that the financial services industry is extremely aware of exactly those facts. They're very aware that their consumers want privacy, want security, want accuracy absolutely assured. They’re aware of it and because they're aware of it they demand it from us as their service infrastructure provider.

The issue that is really complex is the fact that while consumers demand almost perfect accuracy, security and privacy, at the same time their challenge back to us is I want all of that, I want it perfect, I want it complete. I’ll tell anybody who calls me and asks me about it that that’s what I want. I want it in total and I want it complete.

And then they’ll tell us, the service providers, but by the way, I only want to use one password and I only want to use it once. And don’t do anything that gets in my way from getting all of these services automatically and, in fact, why aren’t you doing more for me. And don't give me more things to do online; give the online services you’re doing the ability to do more things for me.

It is a very real issue, and the issue, I think, that is the most concerning to us when anything like this hits the radar screens here in Washington and you have people that are not in business and are not dealing with these consumers in a real-life business application, is that it is very easy to oversimplify the issue and decide that what you want to do is pass laws to try to provide perfect security just based on the reply that a consumer gives to a simple question.

In reality it’s a very complex issue and that is consumers want privacy and security but they want no extra work and they do not want what you do to get in the way of the services that they demand that we provide.

What you have in our industry, the financial services industry, is a very strong, probably the strongest implementation of what John was just talking about and that is the banking industry in the United States believes, and in my personal opinion they are accurate in this belief, that they exist today based on one constant and that is they have consumer trust.

Over a hundred years -- while all of us love to complain about our bank because it’s part of the national pastime -- when push comes to shove and you need some place to secure your money you go to a bank.

The fact is today in this digital world you can manage your finances almost anywhere with almost anyone and as we go more online and as more gets digitized you're going to be able to have even greater freedom.

But the fact is the banks are still by far, and by banks I’m using a broad definition that includes investment firms because that line obviously is clearly no longer a line, what we trust, those trusted names, the financial institutions, and we trust them because, quite frankly, while they haven’t provided the greatest kind of service we want when we go in and stand in a teller line and try to get the loan approved quickly and that sort of thing, they have been very good at securing our trust. They don't lose our money and they don't share information. They don't allow data to get out easily. They are very, very focused on this issue.

As a service provider I can tell you that in the thousands of contracts we have with the thousands of financial institutions that we serve, every single agreement that we have has built into it the absolute requirement that we secure the privacy, security and accuracy of the consumer's financial information.

We very much need to be able to keep that kind of trust. We very much need to be able to figure out how to continue to improve that process, but at the same time what we cannot have is impairment in our ability to be able to provide that kind of improved security and privacy which means we need access to information.

One of the critical things that we have to do when someone goes online and signs on to a new online financial service is we very much need to have the best possible way we can to authenticate that that person who wants to go online and access this information is indeed that person.

If we’re the front line in why people care so much about identity theft, the only way that we do things is accurately, and I can tell you we do it very well today. We’ve improved tremendously almost on a twelve-month basis.

Each new release of the systems that we have put out always has significant improvements in our ability to authenticate and our ability to ensure privacy and our ability to secure the accuracy of the system.

But that authentication capability is absolutely dependent upon the kinds of information that we have to

critical and as personal as you can get and the industry is absolutely focused on making sure that we continue to earn the trust that the industry has earned over the last hundred years.

So in conclusion, our experience is that this is a very complex issue. It’s extremely important. It’s very important to consumers and they want it, but it’s a complex issue.

The idea of individual states making snap decisions and fragmented decisions on these kinds of issues so that we can’t provide the same level of service across the United States and the idea that questions are being oversimplified so that the solutions become oversimplified and end up getting in our way of being able to provide the kind of privacy consumers want are the kinds of things that concern us.

We believe very much that meetings like this are very important because at the end this is a complex issue that needs to be well understood. The full perspective of what consumers in the United States really want, the full understanding of what they really want is important and ultimately we need all of that understanding to be able to make wise, informed decisions.

MR. SEIFF: I apologize. If you want to interrupt any time just go right ahead. First, let me start by saying I absolutely agree with everything Pete said. My conversation today will be a little bit different.

Number one, I want to tell a little story about last summer. I love and am a slave to convenience.

My book reading habits have changed since Amazon came into the world; it has just made it so much easier and so much more convenient to shop for books that I have become a slave to one-click shopping and have probably doubled my consumption of books in the last two or three years.

Last summer I went on to buy a book and I was in my shopping cart and there were 34 Disney books in my shopping cart. And so I picked up the phone and I’m just buying my little book and I call my wife and I said, do we really need all these Disney books, what was going on. And she said I have no idea what you're talking about.

So I put two and two together. I went home. I sat down with my four-year-old son. And he doesn't know how to read or write. And I said, Reed, do you know -- that’s his name, Reed -- do you know how to get to Amazon? And he said, yes, Dad. Let me show you.

I had set up for him, because I'm teaching him link. It took him to an affiliate program at Amazon and he learned how, by playing around, to put books in the shopping cart.

For some freak reason my one-click shopping had been turned off at home. If not, I would have found out by having 34 books delivered to my door. So I have left it disabled at home and continue to have it enabled in the office. And so while trust and security and accuracy and privacy are the pillars for sound business decisions they are not enough. We need to give consumers choice.

What I want to talk about today is what choice means and how it impacts companies like Bluefly. And just to give you a little bit of background, Bluefly was started five years ago. We sell men's and women's fashion. We did about $30 million last year selling brands like Prada, Polo, Armani, Gucci and Diesel.

Our average retail prices are about 60 percent off of store prices. We buy the stock six or eight weeks or sometimes the end of the season and my guess is most of you have never heard of us. So the ability to reach out to you is fundamental to our success as a company over the long term. And we have invested over $60 million in building a secure and accurate system and also reaching out to consumers over the last five years.

What Bluefly -- and I apologize for taking some on this but I think it’s helpful in understanding how we want to use information to fill this concept. What Bluefly is trying to do is be the best of all retail worlds. It is trying to be the first place where you can get the selection of Bloomingdale's and Neiman’s, the savings of a Lohmann’s or a T.J. Maxx, the service of a Nordstrom or a Land’s End and the convenience of a J. Crew.

Basically, what we would like to do is take the traditional off-price store experience where you dig through racks and bins and make it much simpler, much nicer. Sit on your couch, have a cup of cappuccino and we’ll find you what you want to see.

This is what the women's department looks like today. We’re in a little more promotional mode than normal but we put stuff together, outfits for summer fun. We have Diesel starting at $19.95. We have Fendi and Michael Korr and Prada and Polo on the site. And without turning this into an advertisement I just wanted to give you a little bit of the picture of what we do.

Consumers don't need more stores. This country is already overstored. The service levels are, at best, acceptable and at worst inconsistent and unacceptable. And when you want to save money, which I certainly do and I assume there are several of you here who would like to, it’s not always the easiest thing to do.

It’s inconvenient either because the average trip to the mall is over two hours round trip or because when you go to an off-price store to shop for savings you have to dig through racks and bins. So the convenience level is not comparable to going to The Gap, for example.

Our ability to compete as a start-up fundamentally hinges on, among other things, the creative use of information because by using that information we can create a better experience and a better option for consumers. And not surprisingly it includes our chance to succeed as a company.

If we win, in my humble opinion, consumers get a new hybrid form of retail. Our brands may not appeal to everyone. Our savings may not appeal to everyone. Our service may not appeal to everyone but we are creating a very strong and small following amongst our customer base and we’d like to expand that.

Our suppliers win also because we pay more for product because we’re presenting and selling it in a different format. As a consequence their business economics can and should change because they recover more money from their excess inventory and our economy, in theory, with thousands and millions of businesses like ours would improve as well.

We, this year, employed 80 people. This business didn’t exist five years ago. In the last five years we've invested over $60 million in people, infrastructure and marketing.

Here are some examples of companies that I like that use information to my advantage. Number one, I talked about Amazon. I do love one-click shopping. But even more than that, I love knowing when an author that I like releases a new book before it’s released so I can pre-order it and not have to check in the bookstores when the next Nelson DeMille book is coming out.

I like going into a hotel. Last night I did not have to give any information other than my credit card. I got my king size bed and no smoking room and they didn’t need to ask for anything at the check in.

And I like having caller ID. There is nothing more annoying than having a call while I’m having dinner and I’ve gotten them on my cell phone at home on Saturdays. And I am so protective of my information.

So I appreciate the two sides to this issue but responsible businesses don’t do that. And they shouldn’t be allowed to do that. So I am, I hope, have a balanced perspective on this, both as a business owner and as a consumer.

I’ll give you an example of how we intend to use information. If you go to look at women’s pants at Bluefly we have over one thousand different styles of pants and that’s probably too many, and why we’re running the business like that is something we’re going to change. But I would like to offer hundreds of pairs of pants, probably not a thousand in the future.

What I would like to be able to do for each customer over the next 12 months is identify, based on the brands they've clicked on in their previous site visits or even during that session which brands they are most likely to be interested in, which price points they’re most likely to favor and then present the thousand pairs of pants to them in the sequence that is most likely to interest them.

So sure, the company benefits, but the consumer benefits too for not having to fill out forms, for not having to dig through all of the thousand pairs of pants.

This is how we present it. Here there’s only 63 products. There’s seven pages of nine products but you can see that with a thousand pairs of pants it’s a 100 pages of information that can be dug through by brand, by category, by price, sorted by what is new.

Off-price retailers can’t buy everything in every size because by definition we buy end-of-season stock. Bluefly can remember the size you wear provided we continue to be allowed to so that we, if you choose to let us, will only show you product that is available in your size.

That significantly reduces the level of frustration and we measure this. We actually take customer satisfaction surveys and we get a chance to see how this sizing information impacts the customer.

The benefit to us, of course, is it allows us to be more successful economically and therefore continue to build more services and more features for the consumer.

Faster check-out. We've all been through this online. It remembers everything for you. You don't need to fill it out. And in our case we speed check-out to two screens, a preview screen and then a final place-your-order screen. My son still hasn't figured out how to break that one.

This is one of my last two points. Just the simple fact of knowing your ZIP code will allow us to provide services. When it's raining, how about an umbrella and a raincoat on the home page for you.

If there's a heat wave and you're in Maine in November and you need some short-sleeved shirts and it's 80 degrees, and I have been in Maine at 80 degrees in November, we could provide that level of service.

If you live in Chile customers can provide a service for us. We have winter coats in April, how about taking some of them off our hands at a great price. And perhaps even sequencing product based on what other people in your ZIP code like, in effect, aggregating information to provide that.

The last point I'll make is even traditional concepts help new companies. The ability to buy names, to prospect, improves the economics of our business. It allows customers who have never heard of us to find out about us which we think is a service. It helps us acquire profitable customers.

We can even buy keywords on the Internet so when someone types in Prada a Bluefly ad can appear. That kind of use of information can fundamentally alter the economics of our business over the next five years.

I'll just hit the highlights of this. Four percent of our customers generate 49 percent of our profits. Understanding who those customers are allows us to pick the products we sell to them. It allows us to target market more effectively. It allows us to understand what level of service we can provide for our customers as a whole and has, in fact, allowed us to identify many new strategic opportunities for our business. Thank you.

COMMISSIONER MURIS: Thank you very much, Ken. And finally, Tom.

MR. SEDDON: Thank you. Well, I guess moving from from a business that is all clicks I'm very happy to be here in a business that is really all about bricks. As opposed to many of the other panelists, we really, in the hotels business, are the end-users for a lot of the types of things you have heard about, particularly from the first two gentlemen.

Our company, InterContinental Hotels Group is the world's most global hotel company. We operate InterContinental, Crowne Plaza, Holiday Inn, Holiday Inn Express and Staybridge Suites Hotels. We have about 3300 hotels in just about a hundred countries around the world. And every night we accommodate about half a million people which means during a typical year we have got about 150 million guests choosing to stay with us. And that really adds up to an awful lot of information. When I say we're a bricks business one of the interesting things though, I think, is just how dependent on the free flow of information our industry is.

Like I said, we are a very global business and while the actual act of being in the hotel and staying and sleeping in the night is something that is very straightforward and has been around for thousands of years a lot of things to do with the process of making that reservation and making that reservation easy for you and making sure that when you show up at our hotel we know what you like, as Ken was talking about, are absolutely dependent on information.

One of the critical things for us as a business is to be able to flow information not only between countries and within countries but also between businesses. The hotel industry is extremely, or the travel industry in general is extremely effective in terms of exploiting a network of interdependent partners.

So, for example, if you choose to make a booking on Expedia for a Holiday Inn Hotel, that booking goes through Expedia’s system and you’re providing them some information. They need to get that information to us. What we will do is put that into a centralized database that we will then push out to the individual hotel so that information is transferring between businesses.

And one of the things that isn’t immediately apparent to people is the extent to which even inside what you might consider just our business we actually have a number of partners. About 80 percent of our hotels are actually franchised.

So we don't own and operate the majority of our hotels. The majority of our hotels are actually owned and operated by entrepreneurs, third-party businesses that, for all legal purposes, are separate entities to us.

Yet, from the customer’s point of view they see it as part of the overall brand. And it’s also very important to us that each of those properties does appear to the customer as part of the overall brand.

But I need to transfer all of the customer's information between my business and that hotel there which actually may be owned and operated by a completely separate company within our standards and operating to our rules which do include things like standards on privacy and security.

So when you choose to make a booking and you maybe phone up our reservation number, you're sitting in Germany, and you may be talking to a reservation center that's based in Amsterdam. That reservation center in at night and check in immediately, which is one of the biggest bugbears in the hotel business.

When you show up at a hotel, like I did, at midnight last night you do not want to be standing around for five minutes telling them again what your home address is and what type of room you like and especially when you say, well, I’ve been here ten times in the last three months, perhaps you might know that. I’ve been to your hotel brand 50 times in the last six months and perhaps you really should kind of start to get to know me. So we really do need to be able to facilitate that information flow and it really has a huge value to customers.

About one-third of our business comes from

And that's a great way for us to hold the information about preference and credit card on file so that if you're a frequency program member you can show up at virtually any of our hotels in the world having made your booking, they will have a key packet pre-made up for you.

So you walk up to the front desk, say I'm Tom Seddon, here's my identification and they'll give you the key packet and then you walk to your room which is about as good a reservation and check-in experience as you can possibly get. And that's really where we are trying to go.

So people really do value the benefits they get from the smooth reservation process, from our ability to make that available everywhere that they want to be, whether it's online, whether it's through a travel agent system, whether it's through an 800 number, whether it's calling the hotel direct, they need to be able to have a very seamless process there.

And we have invested very large amounts of money in facilitating that process and making sure that process is secure and is something that people feel they can trust, because our brands are really all about trust. If you think about our business, Holiday Inn has been around for over 50 years. InterContinental brand has been around for over 50 years.

And so it is very important to us to maintain the value of the brands to customers for the next 50 years. We don't believe that it is right, for example, for us to sell our customer information or rent our customer information. That customer information is the lifeblood of our business.

We consider that both a trust from customers and also a hugely valuable asset. And so it's both in our narrow economic self-interest and the right thing to do to make sure we do everything we possibly can to protect that. And it's very, very critical.

We do actually use the information for a lot of marketing purposes as well. And we are big customers of services like Acxiom provides in terms of making sure that information is very accurate.

We probably mail out something like 50 million pieces a year mostly to people who are part of our frequency program in terms of statements, et cetera, and who is not. And that allows us to dramatically reduce the amount of outbound mailing, for example, because I don't want to waste my time and I don't want to waste my money communicating with customers who have demonstrated they're kind of not interested in the communication I'm sending to them.

On the other hand, there's a great segment of customers who really like the offers that we send them and we are increasingly able to customize the offers. So, for example, based on your past behavior, based on what I know, for example, about the ZIP code perhaps that you live in, I might send you an offer that's more family targeted or I might send you an offer that's more targeted to a couples breakaway or I might send you an offer that's more targeted for just a business trip.

And again, increasing my ability to target means that I'm less likely to send something that you just look at and think, I have no idea why they sent me this and throw it in the bin. So we have a very strong interest even on the marketing side of things to make sure that our information is used really well and to a large extent it's all about reducing unwanted contacts with customers, unnecessary contacts with customers.

So overall, I think the big thing from our company’s point of view particularly is ensuring that we do get free global flow of information. That is something where we have been on the front end of experiencing, for example, the European Union’s(EU) approaches and particularly some of the fragmentation there and the lack of clarity which makes it very difficult then to make sure that you are complying with what is being required.

And to a large extent we generally feel that just good common sense is what drives it anyway because we are in the business of keeping customers happy. We’re in the business of keeping customers. That’s what it’s all about.

The hotel business is an extraordinarily competitive business and so we really, really have to be very focused on the information that we use and generally feel like the ability to transmit that information absolutely is in the customer’s interest. And the fact that so many customers so willingly give us so much information kind of demonstrates that.

And we feel that we need to make sure that in the interest of maintaining a healthy business going forward that there is nothing that impedes that flow, either directly or inadvertently.

COMMISSIONER MURIS: Thank you very much, Tom. There have been several very interesting points here and I want to start a general discussion about some issues. And let me start with the issue of the incentives that you all have to make sure the information is accurate and kept private.

I guess one way to put this is what is the return on investment for companies to use their information in a way that consumers would consider responsible? Let me start with Pete.

MR. KIGHT: I've got the easiest answer to that, I think. The incentive for us in taking care of consumer privacy and managing that information is our continued existence. We, a long time before this became the big issue, had to decide early on, because as you can imagine in our systems, with more than 10 million consumer households managing their finances through our systems we have a lot of information.

And we had to make a decision early on whether we thought that information was ours and which you would need to decide if you thought you could resell it or do something with it. And we came up with the novel concept of asking the consumers who actually put in the information, who do you think owns this information.

And it was not a shock to us to hear them say well, we do and you don't. So our return on managing this is pretty absolute and that is the consumer has said quite

by that lack of trust.

So in our world we think creating a loyal, long-lasting relationship bears itself out in lower cost to serve and more revenue on the back end. So it’s awfully, awfully important that we manage the information that we have that hopefully over time engenders the kind of loyalty we want out of our customers.

MR. SEIFF: Can I add one thing to that?

COMMISSIONER MURIS: Sure.

MR. SEIFF: This is a binary issue. Trust is the foundation for a successful business. And I would hate to be an auto dealer. Can you imagine what goes on, having nothing to do with privacy issues, but if you imagine what goes on when a customer walks into an auto dealership they are so skeptical of what they are going to be told and what they are going to be sold that the hurdle that needs to be overcome is insurmountable.

Running a retail store I want my customer coming in and saying this place has credibility to me. I trust that when they’re pushing product they are not pushing their weak product but they’re pushing their best product and, in fact, that is a business decision we have made, to engender more trust.

And I trust that when I give them something they are undertaking a fiduciary relationship with that information. We operate that way. That is not even a topic of conversation or debate in my organization and I have never met a good company in this country in all the conversations we have where this is not a binary issue.

You protect that information with the integrity and perhaps even higher than you would your own. I give my credit card out to my assistant all the time. I would never think of doing something like with someone else's credit card, even if it was my wife’s because we protect other people's information with a higher fiduciary standard.

COMMISSIONER MURIS: Charles, did you want to --

MR. MORG:ynnnnnn dard.

Early on, you know, Jennifer Barrett was named chief privacy officer in 1990, and I think one of the first in the country, because we wanted to really understand this concept of privacy and data use and keep it as one of the core concepts and principles that guided our business's development.

It was so important to us that we made it one of the core functions in our business and it remains that today. And for the last five years Jennifer and a staff does nothing else but deal with this issue, privacy and data use and maintaining these trusted relationships.

COMMISSIONER MURIS: Thank you. Tom, did you want to add anything?

MR. SEDDON: Again I would absolutely echo what everybody has said about the importance of trust. Our company depends on the value of its brands and the brands are only as good as what customers think about them. So we are always extremely concerned to make sure we do nothing to damage the value of those brands in people's minds.

If you think about our hotels do about $10 billion of revenue a year, the real estate backing them up is worth about $30 billion. So there is so much money tied up in the brands. There's so much money tied up in what the brands mean in terms of the real estate that the protection of that customer franchise has enormous economic value to us.

It is something that we place a huge amount of importance on, not only in terms of some of the high-tech stuff but even down to something as simple as one of our simple, most basic, global standards. In every hotel we have, everywhere in the world, when you walk up to the front desk and the front desk person hands you your key they should never, ever say your room number aloud. Very simple, absolute bedrock standard for us.

So they should write it on the thing, give it to you, because even the act of saying your room number aloud at the front desk where someone else might hear it we consider a completely outrageous violation of privacy.

So it's everything from the most complicated network protection consideration down to something as simple as front desk training and making sure that you never ever say a guest's room number aloud, because we have so much money tied up in making sure that we never break that trust.

COMMISSIONER MURIS: Let me ask a question and I think I'd probably like to start with Charles about accuracy versus predictability and maybe versus is the entirely wrong word but I suspect there are some trade-offs there somewhere. Is predictive really what you're getting at? Is there some difference?

MR. MORGAN: Yes, there is quite a bit of difference. I would say that accurate data is by far more predictive however, so that those two concepts are related, very much so. If you have a lot of inaccurate data you're going to get inaccurate predictions or at least less precise predictions. Even inaccurate data has some predictive value but it's not nearly as good as accurate data.

But also inaccurate data costs us when we're trying to link data -- we're talking about hotel data -- what if we misconnect customers, and we're talking about just in the hotel example, inaccurate data and you start giving somebody who is a nonsmoker a smoking preference and all of a sudden they say what do you mean? I've been a customer.

Well, inaccurate data can create customer relationship problems. You target people with very inappropriate kinds of things or you target people that have asked to be opted out -- they may be a good customer of yours but you start mailing to them because your suppression process isn't good.

Inaccurate data can kill you in so many ways. You can be trying to create a better customer experience, as at Bluefly, and if you mistarget you can actually create a bad customer experience. So inaccurate data can hurt you in a lot of ways, not the least of which is if you mail to somebody at an address they don’t currently occupy it is a ignore your communications.

The economic impact of this is so profound that even if we weren’t all up here saying we want to be good citizens, we all want to run good businesses. And so the powerful economic driver here is build the trust, keep the information accurate and the company will be rewarded through higher levels of trust and better performance with whatever communication or whatever marketing tools you use.

COMMISSIONER MURIS: The four percent that you mentioned, do you do something special to get more data from them other than that they make more purchases?

MR. SEIFF: We haven't treated them differently on the data capture side yet. We’re still an evolving business. We put every customer into quadrants in terms of profitability and just as an aggregate number in terms of profitability and revenue generation.

What we discovered is when you match that quadrant against the brands that our least profitable customers buy and our most profitable customers don’t buy we could eliminate millions of dollars of inventory investment that we didn’t need.

So that kind of information so far has been used for merchandising and marketing more than it has been in terms of approaching it from a segmentation of data capture.

lot, you tend to go back to a lot of the same places all the time.

So rather than going through the brain damage of trying to figure out from your behavior what your favorite, where you might like to go, we just kind of said would you like to tell us. And surprise, surprise, we have probably, I think, well over a million customers now who have already put their list of their four or five hotels.

So they go to the website. Instead of drilling through I want to go to Atlanta and now look at the 30 hotels and find the one I want and the room, it’s just like click again, repopulate basically exactly what you booked last time and you say that’s what I want again. Thank you.

It’s a whole lot easier we find to keep information accurate and it’s a whole lot more predictive when you’re working with stuff that customers actually care about. So that’s generally our big approach.

MR. MORGAN: Can I jump in here? I know you like data so let me give you some data from 18 different travel and entertainment customers of Acxiom that was submitted from their customer prospect files.

Interestingly enough, we found about 6 percent duplicates on those files but slightly more disturbing were 1.44 percent deceased. I think the point here is there’s a lot of change and it’s not simple to keep that data accurate even if you try as hard as you can.

MR. SEDDON: Absolutely not. And we don’t want to keep data that is not useful and is not accurate because it’s just you have a huge amount of overhead then associated with hanging onto that. So we try to be pretty mindful about not picking stuff up that isn’t useful.

COMMISSIONER MURIS: John?

MR. THOMPSON: Well, our system depends upon customer participation in ensuring the accuracy of the data because we run an alerting service about Internet threats. It’s important that customers tell us how they want to be contacted, when they want to be contacted, and what kind of information they want us to contact them about.

Hence, if a new threat emerges on the Internet and if you want to be paged by e-mail about it, any time your pager number changes, if you don't tell us what that is, you are not likely to be alerted in the manner in which you expect it. If your e-mail address changes you’re not likely to get an e-mail alert from us.

So it’s awfully, awfully important that our customers participate in the process of keeping the information fresh. And hence, we do an awful lot to make sure that that is the case because in many instances an alert in advance of an outbreak by a matter of days, if not hours, can prevent a disastrous network effect for one of our customers and hence the alerting process and the accuracy of the information that underpins that is critically important.

COMMISSIONER MURIS: Pete?

MR. KIGHT: The only thing I think new that I would add to that, is your question further clarifies the issue of why this is more complex than some of the oversimplistic approaches that you read about. Our customers demand near-perfect accuracy and near-perfect predictability and they simply won't accept anything else.

This is much more complex than solving this with an opt in, opt out type of approach. In essence, an opt in, opt out type of approach like some of the oversimplistic ones I’ve seen would leave us in a position of saying to that customer when they log in and we need to authenticate them, would you like to be authenticated well or would you not like to have the authentication go very well and we’ll take a guess because I need your Social Security number if I want to do 3.06 Sigma level authorization. It doesn't work like that. You can't opt in, opt out. It’s just much more complex than that.

One other thing I would add because being as a business person, especially if you have the title CEO, these days you sort of sit up here and listen to all these CEOs and you realize nobody is going to trust us right now when we talk about how you should trust us.

We talk about all this trust. Now, all of us have pointed out that we have to understand that people need to trust us if we want to stay in business. We're not asking you to trust us because we're good people; because we have CEO titles you assume we're not. We're saying you need to trust us because we understand that that is what customers absolutely require if we want to stay in business.

One of the issues that's vastly overlooked in this whole discussion is the digitization of information that has brought up this whole privacy issue. At the same time what's coming along is business is becoming more and more digitized and the information flow more free; the velocity of choice that is going to consumers is accelerating dramatically.

By velocity of choice I mean in today's world and even greater in tomorrow's world if you don't like the way it’s also giving the consumer immensely more control over their own destiny. If you don't earn their trust they can change you with the press of a button. And, in fact, even in Tom’s case, as he’s pointed out, he’s now doing so much business online that they can change him with the press of a button and just pick a new favorite hotel if he doesn't earn their trust.

So consumers are actually gaining a lot of power out of this whole process but what you’re reading about is just one side of the issue.

COMMISSIONER MURIS: We’ve got time for another question and let me start with Tom. What would it mean if exchanges of consumer information were prohibited. I mean, would public data like census data be useful and what would the impact be on consumers?

MR. SEDDON: Well, for us, if we were not able to exchange data, let’s take an extreme example and say we couldn’t exchange data with any other kind of company, any other separate legal entity. That would basically mean that no hotel company in the world, no travel company in the world would be able to take your booking. You would basically have to. Contact the individual endpoint.

The hotel business would go back to before 1958, I think, when we came out with the first centralized reservation system, Holidex, and the concept of an 800 number you could call for any hotel.

So you would go back to if I want to go to Washington I've got to get the phone number of the specific hotel in Washington that I want to book and I have to call them up and that hotel has got to keep a little list right there with their own little database that they can't share with anybody.

If you went to one Holiday Inn, and had a preference for a nonsmoking room and then went to another Holiday Inn they would not be able to know that you liked a nonsmoking room. You would have to keep giving people your same information again and again and again.

I think it would really basically eliminate a lot of the convenience that has developed and a lot of the things we totally take for granted in terms of the ease with which, particularly in the travel business, you can book and conduct travel. If you think back to the way hotels were in the 1920s, that's really where we'd be back to.

COMMISSIONER MURIS: If it was an opt-in world and people had to every time or at least initially take the time to give you the permission to use their information in the future would that work or is that what you do now?

MR. SEDDON: It's kind of what we do now. To a very large extent most of the things we do now are opt in,

It would be a tremendous barrier to entrepreneurial startup businesses and the formation and growth of the business. You know, the jobs in this country come from small business. We would definitely slow that process down significantly.

COMMISSIONER MURIS: Pete?

MR. KIGHT: In terms of financial services, I guess the one point I would make is ironically the more you impair the basic ability to double check financial information with authorization what you do is significantly reduce our ability to secure privacy and security.

So, in fact, again back to the issue of it’s very complex. If you put the wrong rules in place so that we can't exchange the right kind of information, I can’t provide you with the privacy that secures your information.

COMMISSIONER MURIS: Ken?

MR. SEIFF: If I could presume to speak on behalf of startups and small companies, when you start a business there is only thing you need and that's customers. It's hard enough already to start a small business. We’ve spent $60 million, as I said before, starting a small company.

I hope it works and it becomes a big company but impede that any more and we would not have been a survivor of the Internet bust. And I think it's only getting tougher now.

I'll be interested to see what happens with the spam regulations. I have a feeling they’re going to hurt good companies and not do anything to the bad companies no matter how well crafted the legislation is.

This opt in, opt out is a huge issue and I don't want to presume to even set a standard for what opt in means or what opt out means but we have found the shift from going to opt in to opt out is dramatic and, in effect, as long as the customer still retains control of what they're doing and what we can do with that information I don't think there’s a great difference to the consumer but there is a huge economic impact to businesses.

I would say on behalf of small businesses, please don't shut us down from acquiring new customers entirely. We're happy to operate responsibly and follow any guidelines that come from the government on this front. I think we would be very supportive of guidelines as long as they allow us to continue to stay in business.

COMMISSIONER MURIS: Our time is up. I wanted to thank everyone and I’m just sitting here thinking of the opportunity cost of all of your time to be here. Unlike when we have lawyers in front of us whose opportunity costs are a lot less than yours, at least in terms of real impact on the economy, I very much appreciate your time and I would appreciate all joining in giving you a round of applause.

(Applause.)

COMMISSIONER MURIS: We'll reconvene at 10:15 for Commissioner Swindle.

(Whereupon, a short recess was taken.)

COMMISSIONER SWINDLE: That was a great first session. I was impressed with it and I hope you appreciated it as well. I hope the rest of the day will be the same.

The first thing I'd like to do is thank Maureen Ohlhausen for her coordination of this event and all the staff that worked on it. I believe that probably one of the best things we do at the Federal Trade Commission comes for us. We really appreciate John Thompson of Symantec, Pete Kight of CheckFree, Tom Seddon of InterContinental, Ken Seiff of Bluefly and Charles Morgan of Acxiom for being with us.

We're taking an incredibly important first step, I think, in trying to bring forward the concept of cost and benefits in information flow and the importance that that information flow plays in our economy in a macro sense, and certainly as Ken was pointing out in a micro sense for up and coming businesses. If we do the wrong thing with legislation and policy we can really cause some problems.

I particularly appreciated Pete Kight's reference to the often, too often used concept of oversimplicity. I could not help but agree as he was talking about the problems that we face when we sometimes take very complex problems and try to oversimplify them and then legislate based on that.

So much of what happens in this country is driven, at least in the legislative process, by an emotional reaction to something we perceive as good or bad and that we have to do something about. And oftentimes for expediency purposes we do tend to oversimplify in the legislature, both state and federal; we say okay, let's pass something. We've done our job. Problem solved, let's go to the next problem.

Oftentimes we have actually just laid down a much worse problem. I couldn’t help but think of the conversation I had with Jeff Bezos a couple of years ago out at a conference out at Aspen.

He told the story about when they first got Amazon going they had no idea that this thing would really take off and they were operating, if I recall correctly, out of his mother’s home, actually her garage, and they were getting the books shipped in to them and they were filling a few orders.

And all of a sudden it started to pick up and they were wrapping the books in something like Saran Wrap on the floor of the garage and, you know, eventually they were going seven days a week, 24 hours a day. They’re down on their knees wrapping these books.

And Jeff says, you know, it was getting painful. Our knees were getting bloody and he said finally, it just occurred to me like a flash of light coming: I stood up and said, guys, you know what we need? We need some knee

19

goods and services, and as was mentioned, the instant increase in choices.

I was marveling at Pete’s comment also that in the near future you'll be able to change your credit services by the mere punch of a button. You know, have any of you changed your long distance service provider recently?

I hope when we get to that point that the punch of a button works better than that process because that’s not a one button punch. That’s sometimes days and weeks of getting it straightened out.

Consumer concerns about the privacy of personal data as reflected by every one of these very senior officials, most CEOs, is that it’s also very important to those business.

All of the consumers’ concerns have to be respected by businesses. And we’ve got to work together to ensure that our approach both protects privacy and preserves the important benefits of this information flow for our society, our economy and consumers and literally to the world economy because that is where we’re going.

Today’s workshop is about finding the best policy solutions based on facts and data, so I say to our panelists today, and we’ve got another distinguished group here, check your anecdotes at the door. To rephrase a memorable line from the movie Jerry Maguire, show me your data.

The Commission testified last month that the FCRA, the Financial Credit Reporting Act, helps make possible the vitality of the modern consumer market providing a carefully balanced framework giving us the benefits that result from the free, fair and accurate flow of consumer data.

To my friends who support the reauthorization of that legislation, the Fair Credit Reporting Act, show us the data. To my friends who oppose reauthorizing the Fair Credit Reporting Act, show us the data. Your data, and particularly if you oppose it, is especially important since you have the burden of showing why we need a change in the way it already exists.

Putting facts on the table informs policy makers. It informs those of us in the regulation business. It informs d framewtredit Reporting Act, shokDa7rtT, show us

(Applause.)

MS. TWOHIG: Good morning everyone. I’m pleased to have the opportunity to moderate this discussion by such distinguished panelists. The purpose of the panel is to discuss more specifically the costs and benefits of information flows used in credit transactions.

We have a lot of ground to cover, so I want to get started right away. Our panel represents an impressive amount of experience dealing with credit information issues from all kinds of perspectives. They will each present brief remarks with the hope that we can get to questions and a discussion at the end of some more specific issues. Our first speaker is Fred Cate, distinguished professor of Law from Indiana University.

Next, we’ll hear from Pete McCorkell who is senior counsel at Wells Fargo. Then we’ll hear from Bill Gossett who is president of Islands Community Bank in South Carolina. Then we have Andrea Fike, Vice President, General Counsel and Secretary of Fair Isaac.

Then we have Laura Desoto who is senior Vice President at Experian. And then we’ll hear from Travis Plunkett, Legislative Director at Consumer Federation of America and finally from Evan Hendricks who is Editor and Publisher or Privacy Times. And without further ado we’d like to get started with Fred Cate.

MR. CATE: Thank you very much. I very much appreciate the chance to be here. I appreciate the fact that the Commission is hosting this. It’s difficult to imagine a more important topic and the opportunity for a more thoughtful discussion of it than in the sort of political highlight of Capitol Hill hearings. It’s something we are all particularly grateful for.

I have been asked to try to set the groundwork for all of the panelists by talking briefly about credit reporting generally before turning to more of the topic of the impact of credit reporting.

Credit reporting, as certainly the vast majority of you know, is a tremendous volume business. 200 million individual credit files are maintained by the three national credit reporting agencies.

One and a half billion separate credit accounts are reflected in those files, and in many ways it’s much more accurate to think of files in terms of accounts because all a file is is linking together disparate account data. Credit accounts include updates of 2 billion items of trade line information a month, 2 million public record items a month, and 2 million credit reports a day.

Now, the content of credit reports is actually quite simple and often widely misunderstood. They include identification information, information on open trade lines, basic information on outstanding balance, credit limits, date account opened, payment history and so forth.

Additionally included are public record data, information on bankruptcies or legal collection and other collections information, and then finally inquiries on the credit file, including the date and identity of the inquirer for the past two years.

Information not found in credit reports would include employment information, income, race, other lifestyle indicators. Credit scores, for example, is something that credit bureaus are often being asked to change or disclose, but they don’t have them.

Other thaTDmc(they don’t have them.)Tj/F1 1 Tinoration ct

9

Oedi2ing that credit bureaus are often being 1 egoTT2 :T

order.

I want to just touch on one other in some greater detail. One of the permitted purposes is for prescreening. And this, of course, is very much at the center of the current legislative debate over FCRA. Prescreening of credit information for the purpose of marketing firm offers of credit or insurance conditioned, of course, on having an opt out system.

As you know, as of 2001, we saw just over 5 billion prescreened credit card mailings. So this is a major use of credit reports, and it is the primary way in which new credit accounts are opened in this country. And it is, by all accounts, increasing.

Another use of credit reports is that credit information may be shared among affiliated companies or entities, among persons related by common ownership or affiliated by corporate control.

Again, this is conditioned on there being an opt out opportunity and clear and conspicuous notice to the consumer that the sharing will take place prior to the sharing actually taking place.

Now, let me turn, to conclude, to some of the issues regarding the impact of credit report data. The other panelists are going to address each of these in far greater detail, so I'm going to take advantage of that fact

significantly in interest rates.

And it’s not just an overall economic effect on the interest rate. If you look at the last example there we see revolving credit actually offering a lower interest rate, dropping even when compared with, say, T-bill rates. So that we see this significant impact of the data aggregation here far beyond just the general trend in the economy.

Perhaps most importantly it means more people have access to more credit, and this is incredibly significant. Let me give you an example of why that is, because what it means is that people who would otherwise not receive credit get access to credit, in many instances for the first time.

So, for example, this slide shows the change in the proportion of U.S. households using nonmortgage credit from 1970 when the FCRA was adopted to 2001; what you see is in the lowest quintile by income it’s almost 70 percent, 68 percent increase over this 30-year period. Again, a

Identity verification now required under the USA Patriot Act. Again, likely to become an important use. And making the financial services sector in general more transparent, resilient and subject to legal oversight.

In closing, the quote with which I think you're familiar from the Chairman of the Federal Reserve Board, Alan Greenspan, about the U.S. financial services sector being more transparent and stronger in general as a result of access to this information. So let me stop there. Thank you for your patience.

MS. TWOHIG: Thank you, Fred. Pete.

MR. MCCORKELL: Wells Fargo has sort of the interesting history of having started in the days when being a financial institution meant that you kept money and gold and things like that in safe boxes and vaults and you moved it around by stagecoach. We don't do that anymore. The amount of financial transactions that take place using hard currency or folding money is really pretty trivial compared to the overall economy.

Financial services now is an information business. Basically, this person has a credit of this much, and this person has a debit of this much. It's keeping that information straight is what financial services is all about today.

A number of the speakers on the first panel mentioned the trade-off between security and convenience. That is a tremendous issue for us in the financial services community, and striking that balance right is a continuing challenge.

If you think about credit in particular, I would say you can break down the cost into four basic categories. First, what we call acquisition cost or what probably most of you would think of as marketing cost. And that may be marketing to new customers or acquiring new customers or getting existing customers to use additional products or make more use of the products they already have.

The other three categories are the cost of capital, credit and fraud losses, and finally, operating costs. Again, on the plane I realized that if I had thought a little bit harder before I submitted these slides lower cost of capital and greater amounts of capital being available have all contributed to that increase in competition, in national competition, and greater availability of credit to the people who need it most.

brokers representing separate underwriters. Certainly there are some direct underwriters of insurance, GEICO being a prime example of that.

But most insurance business is done through agents or brokers dealing with nonaffiliated insurance companies. And we sort of follow that pattern at Wells Fargo, although a number of other financial institutions, Citicorp obviously being the most prominent example of that, do have insurance underwriting in the same corporate family.

Wells Fargo, in particular, has a strong focus on cross-selling products to additional customers. We have as a goal to have every customer have eight Wells Fargo products. I will tell you that is a distant goal. We’re not quite halfway there yet.

In my case, they're getting close. I’ve got, by my count, seven different Wells Fargo products and that involves relationships with five different legal entity Wells Fargo affiliates to provide those seven products to me. I don't have anything under the insurance part.

Why do we want to do that? Well, first of all, because we have regular contact with existing customers it is a lot less expensive to get the message out to them about other products and services. We can do that not only when a banking customer comes on the website but also when we send them monthly statements. When they call in to inquire about one product, we can tell them about other products that might be of interest.

Because we know what they have at least with Wells Fargo, we can do a better job of saying what is or is not appropriate for this customer. If somebody already has a Wells Fargo credit card we’re not going to try to sell them another one and if somebody has a pretty large deposit in a Wells Fargo CD we’re not going to try to sell them more deposit products.

We might, indeed, if they come in and say well, I want to put some more money in my CD, we might say, well, gee, you know, you’re earning a whopping 1.2 percent on that right now. Maybe you want to think about a different way of investing that money.

Because we know these people we can do a better job of risk assessment. We can offer them credit at lower rates. Because they already have one product predictably they're going to be more loyal. If they have more than one product, they're likely to stick with both of those relationships for a longer time than somebody who only has one product.

Somebody on the earlier panel mentioned the fact that it's a lot more expensive to have that first transaction with a customer. The same thing is true for

property data is only going to be used in connection with secure products, auto loans, home loans being the primary examples.

The fraud data would include things like the government databases for the Office of Foreign Assets Controls, the Patriot Act compliance, as well as commercially available data on fraud.

The demographic data both in the input and the output is really aggregated information rather than individualized, personalized information. The rest of this information tends to be personally identifiable.

The output from the decision process is a little bit more complicated, because information is going to go into the system of record for whatever account we're talking about. It is also going to go into the customer information system from that process to basically saying Pete McCorkell just opened a new account with us of this type, et cetera, and summary information to be put in that overall customer relationship.

The output from the system of record includes reporting to credit bureaus if this is a credit product, to our own internal hot files or fraud files, and if the need arises, to our collection system. Then those internal hot files, in turn, provide the information that goes back out to external fraud file databases.

Customer information system and again the system of record also feeds into the customer information system as that relationship evolves. Typically between the customer information system and the outside world there is a filter of some kind of marketing database because again, as other speakers mentioned, we don't want to provide any more information to somebody outside of Wells Fargo about our customers than we have to to carry out a particular function.

Also, we have a fiduciary obligation to keep that information private, to only use it for permissible, legitimate purposes; our biggest asset is information about our customers. Again, the demographic databases is aggregate information not personally identifiable.

MS. TWOHIG: Thank you, Pete. That's very helpful and important information and hopefully as we proceed with the discussion you’ll have time to expand on some of those points. Bill?

MR. GOSSETT: Good morning. I’m Bill Gossett. It’s my pleasure to be here. I started in the business of extending credit back in the 1960s. At that time I managed a statewide credit department for a very large bank in Florida.

So in addition to some gray hair I have first-hand knowledge in the use of credit information before things were quite so efficient as they are today, and I also managed the first compliance with the Fair Credit Reporting Act.

Quickly, at that time, we didn’t really have computers as we know them today. We didn’t have calculators. We didn’t have fax machines, if you can remember back then. We did have telephones so our gathering of credit information in our network included upstream banks and downstream banks. If someone needed information from us they would call us. If our customer needed information we would call one of our correspondents and gather that information. That was our method of getting credit data primarily.

The information wasn’t consistent. Whatever the person on the other end deemed was important was what you got. I remember calling the bank in Lakeland, Florida one time and was told that the customer had a seven-figure balance on an account. Well, little did I know that they were counting the two digits to the right of the decimal point.

There was no reasonable method to refute the information if there was an error, on the part of the consumer, the customer. The credit bureaus did exist but remember there were no faxes so if you got a credit bureau to get it in writing, you had to wait for the mail to deliver it or someone took it on a yellow pad and the employee would usually use shorthand and they would abbreviate this that and the other so accuracy and completeness was an issue.

Today we take a lot for granted. In my small bank someone opens an account and before they leave we ask would you like a credit line or an equity line associated with the account in one setting.

My bank has $30 million, the other end of Wells Fargo. We’ve been open just under two years. We're focused on services and we’re an active small business administration(SBA) lender.

My background prior to that included a very large SBA lending bank in the state of Florida. Therefore, my remarks will concentrate on the use of consumer information in the small business context.

SBA tells us that small businesses with less than 500 employees are nearly 98 percent of all employers. They employ half of the private sector and they generate by some estimates up to 80 percent of the new job creation.

So how does Islands Community Bank collect and use consumer information in their small business lending operations? I’ll tell you my world involving credit is rather basic and simple.

The credit report is one major tool we use to

information and through the telephone got very detailed info and were able to make the credit as a result. Again, it’s just a different use of credit information.

We do not share credit report information with anyone nor any other information for that fact that the borrower may provide. We have no affiliates, no third parties and, of course, as our bank matures that is subject to change.

We may use the information as far as financial statements to assess the borrowers other financial needs and across other bank products and services that may be of benefit to the borrower. This would involve any basic banking service, lines of credit, charge card services, mortgages or whatever. Our goal, too, is to always create as full a banking relationship with the small business customer as we can.

So what are the benefits to the bank and the borrowers using the information? First, it allows us to provide credit more cheaply and quickly and to make credit more readily available. Accurate, reliable information about borrowers is essential to our ability to make informed, safe and sound lending decisions.

Credit information speeds up the decision-making and decreases cost of providing credit. In the days before we had a robust credit reporting system it would take bank staff about three days to perhaps a week to gather the information, obtain verification about payment history and other credit relationships provided by the borrower.

This process was not only costly and time-consuming but accuracy is lost when doing a self-investigation. Today we can access good information from the credit bureau in two minutes or less. Credit information, I think, makes credit more available. It helps me to price loans based on the risk or otherwise structure the credit for the risk involved.

Examples would be lowering or increasing the loan to value, requiring additional collateral. I might require an SBA guarantee on the loan if I deemed it necessary in order to make it, or any other number of terms could be altered based on my assessment of the credit risk.

Thus borrowers with lower risk get lower-priced credit and/or more favorable terms, and those with higher risk still get credit albeit at a higher price. Without the ability to adjust price for terms or risk in the face of uncertainty regarding the information I have about the borrower, my choice might be not to make the loan in the first place.

Credit information gives my small bank the ability to compete with large lenders, and I think the more competitors there are and the more quickly lenders can fairly and rapidly access credit worthiness, the greater access borrowers have to competitively priced credit to start or grow a business and achieve economic success.

I think all said, we’re very small. We’re the other end of the spectrum from Wells Fargo but credit information is equally as important to us for our survival on our ability to compete and also the benefit we provide to our customers. I thank you for the opportunity and look forward to comments or questions.

MS. TWOHIG: Thank you, Bill. Just one question before we proceed. You said that you use the information to assess your customers other financial needs, and I assume that’s for your own marketing. Do you also do joint marketing with financial partners?

MR. GOSSETT: Not at this point.

MS. TWOHIG: Thanks. And moving along, Andrea.

MS. FIKE: Good morning. Commissioner Swindle, Ms. Twohig, thank you for the opportunity to participate in this important workshop.

Fair Isaac is the preeminent provider of creative analytics that provide value to people, businesses and industries. Fair Isaac invented statistically-based credit evaluation systems commonly called credit scoring systems and is the world’s leading developer of those systems.

Thousands of credit grantors commonly use scores known as FICO scores generated by Fair-Isaac developed scoring systems implemented at the three national credit bureaus.

A FICO score is a three digit number that tells lenders how likely a borrower is to repay as agreed. FICO scores use information from consumer credit reports to provide a snapshot of credit risk at a particular point in time. Your credit score is a number based on the information in your credit file that shows how likely you are to pay back a loan on time. The higher your score, the less risk you represent.

FICO scores are calculated from a lot of different data in your credit report. This data can be grouped into five categories. The percentages in the chart generally reflect how important each of the categories is in determining your score.

The first category, approximately representing 35 percent of any given FICO score is payment history. The kinds of information included here are account payment information, for example, whether or not you have paid on time every time. If you have not, the amount that has been past due and for how long and how long it has been since you missed a payment.

Also included in this category is information such as the existence or absence of adverse public record information such as bankruptcies, judgments, or liens and the number of accounts on which you have paid as agreed.

The next largest category, representing about 30 percent of any given FICO score is the amounts owed and includes information such as the number of accounts with balances and the proportion being used on credit accounts.

Representing approximately 15 percent of a FICO score is length of credit history. This includes information such as how long it has been since an account was opened and how long it’s been since that account was used.

Representing 10 percent of the FICO score is new credit or really the answer to the question is this consumer looking for more credit. This looks at factors such as the number of recently opened accounts and how long it has been since those accounts were opened. It also looks at the number of recent inquiries on a consumer’s credit record.

Please note, however, that this does not include inquiries made by the consumer to check his or her own credit report. It also does not include prescreening inquiries or inquiries for employment purposes.

The final category, again representing 10 percent of a given FICO score, is the types of credit that are in use and that looks at the balance of a number of various types of accounts such as credit cards, retail accounts, installment loans, mortgages, consumer finance accounts and others.

Although there are many types of information that go into a credit score it is important to remember that no one piece of information alone will determine your credit score. What is important is the mix of this total package of information which, of course, varies from person to person and varies for the same person over time.

FICO scores do not contain factors that are illegal to use in the lending process. FICO scores consider a wide range of information in your credit report but do not consider race, color, religion, national origin, sex or marital status.

And as pointed out by Mr. Cate earlier most of this information is not even included in credit reports which are the source of data from which credit scores are derived.

U.S. law would prohibit credit scoring from considering these facts as well as receipt of public assistance or the exercise of consumer rights under

Where you live is not considered, how much interest you are charged on existing credit accounts is not considered in your FICO score, nor are items that are reported as child and family support obligations or rental agreements.

With credit scoring more people get credit. They get it faster and it is more affordable. People can get loans faster today than ever and that, in part, is due to the availability and use of credit scoring. Instant credit at a retailer, auto dealer over the phone or the Internet would not be possible without credit scoring. As pointed out by an earlier speaker a survey of auto dealers in 2001 revealed that 84 percent of auto loan applicants received a decision within an hour and 23 percent received a decision within 10 minutes.

In the mortgage arena mortgage loans that used to take weeks can now be done in minutes. Credit decisions are fairer. Fair Isaac credit scores transform the economics and efficiencies of credit decisions and allow all relevant information to be brought to bear so that no information that is favorable to an individual is omitted from the decision process.

Credit scoring scientifically and fairly balances and weighs positive information along with any negative information in credit reports. In essence, full credit reporting as you see under the existing version of the Fair Credit Reporting Act and scoring have democratized credit granting. Scoring has transformed credit granting so that it is no longer simply based on who you know.

Among households in the lowest income quintile, the percent with a credit card has increased between 1970 and 2001 from 2 percent to 38 percent. The percentage for minority families has gone from 26 percent in 1983 to 54 percent in 2001.

Even the least advantaged persons in our country have better access to credit today largely in part to the where a judgmental system may not.

More credit is available, more people can get credit regardless of their credit history because credit scores allow lenders to safely assess and account for the risk of consumers who have no existing relationship with that lender, who may not have been in that lender’s branches before or may have been turned away by other lenders in the past.

Lenders who have switched from judgmental systems to scoring have commonly seen that they are able to increase the amount of credit that they can grant from 20 to 30 percent in the number of applicant subjects with no increase in their loss rates.

In addition, overall credit rates are lower.

Scores make credit more afTDms

that lender, redit more afTD ms

lenders in thredit more afTD ms

Lenders who hredit more afTDms

to scoring haredit more afTDms

0p6rkr-nn-and businessen-and the free flow of information permitting such scoring is hugely important to un-all.

MS. TWOHIG: Thank you, Andrea. Credit scoring obviously in-a critical une in credit transactionn-and it is, I know, quite challenging to try to explain it all in the time allotted but we appreciate your presentation. Laura?

MS. DESOTO: I'm Laura Desoto with Experian and I'd like to start with a little background on Experian to give you some foundation for my remarks.

Experian in-a global leader in the information servicen-industry. In North Ar-nica Experian in-comprised of several business units. You probably know Experian as one of the national credit reporting agencien-and you might be familiar also with our direct marketing operations.

We also have a business unit dedicated to helping organizations detect and prevent fraud-and identity theft. I'm here today to talk with you specifically about Experian's efforts in thone regards.

According to sourcen-cited in testimony that I victim assistance.

Fraud is a serious crime. Experian's goal is to help businesses stop fraud before it starts. Experian was a pioneer in fraud prevention providing tools to lenders more than a decade ago to help them identify increased fraud risk.

Early fraud tools like our facts plus system notified lenders of reported variations in addresses, Social Security numbers or other basic identification data in a credit report that indicated increased risk. Later improvements searched for other high risk indicators such as business addresses on a personal credit history and incorporated analysis of less obvious credit report anomalies that suggested need for greater caution.

Today Experian's sophisticated fraud detection and prevention services are not reliant entirely on a credit report. The most effective fraud prevention tools also include data from many other sources and utilize complex analyses.

The tools help businesses verify customer identities. They alert businesses when they are considering an application with information tied to verify fraud activity. They warn businesses of application information that could be fraudulent and fraud tools help businesses assist customers who are fraud victims. The concurrent and continued flow of information and access to a broad range of sources is the foundation on which all fraud prevention tools are built.

Experian's national fraud database is at the forefront of the fight against fraud. It is the first cooperative database of verified fraud information. Members from across industry contribute and have access to information about known fraud activity. A national fraud database report alerts the user when information provided during the application process matches verified fraud records.

When a match is made the business can stop the transaction and take appropriate action. The national fraud database also incorporates complex analysis systems that can identify the level of risk based on the degree to which fraudulent application information matches verified fraud data and differentiates whether the applicant is a perpetrator or a victim. The business then knows to treat the applicant with greater caution or sensitivity.

Detect, our most recently introduced fraud detection tool, adds another layer of defense. The new tool compares application information shared by participants and searches for discrepancies that indicate fraud. Similar to our national fraud database, Detect is a cooperative database to which members share application information rather than information about verified fraud activity.

Information supplied by a consumer in a new application can then be compared to his or her previous application data in the cooperative database. Comparison of application information for subtle and not so subtle differences can reveal attempted fraud otherwise that would have gone undetected.

Coupling insight from the application information of Detect with the verified fraud data of our national fraud database creates one of the most powerful fraud prevention tools available today. The online environment poses its own unique set of challenges to fraud prevention. The most difficult issue is authenticating the identity of a consumer whom a business will never meet face to face.

Experian’s authentication services suite of products verifies the identity of consumers before an online transaction is completed by requiring them to pass an identity quiz.

Questions about basic identifiers such as name and date of birth establish an identity baseline. Such information is known as in-wallet data because it is often found in a lost or stolen wallet. Our authentication services are very successful because they are able to go beyond this in-wallet information by incorporating data from a broad range of sources, credit reports and property records among them.

This information is commonly referred to as out-of-wallet because it is not readily available to identity thieves. Out-of-wallet information is critical for verifying the identity of customers in an online experienced an annual savings of $18 million.

One major U.S. telecommunications company utilizing the combined power of multiple fraud protection tools experienced a 55 percent decrease in losses per handset and decreased the time it took to confirm fraud records by two-thirds.

Clearly, businesses that use our fraud tools will experience significant savings and increased customer satisfaction because the tools help financial institutions stop fraud before it starts.

Similarly, our fraud prevention tools benefit customers with greatly increased risk of financial fraud or identity theft by offering a possible solution to the crime and much faster recovery when a person is victimized.

The key to Experian's fraud services and all fraud prevention tools for that matter, is responsible information use. The most effective fraud tools rely on many data sources to ensure accurate identification.

As identity thieves become more creative in their attempts to commit fraud, the ability of organizations fighting fraud to access and utilize information from a range of sources becomes increasingly important, yet regulators and legislators target that information access in their efforts to attack fraud and identity theft.

That attack is inadvertently aimed at the wrong target and is resulting in friendly fire casualties. We are allies in the fight against fraud. Our enemy is the same.

Unfortunately, regulation and legislation that target access to vital information can critically wound or even kill our efforts to fight fraud. While well intended restrictions on data use and sharing actually exacerbate the problem of identity theft by making it more difficult, if not impossible, for businesses to detect and prevent fraud.

It is essential that in the future we preserve access to a broad spectrum of information sources for use in fraud detection and prevention services if we are to be successful in our fight against fraud and identity theft. Thank you.

MS. TWOHIG: Thank you, Laura and thank you in particular for some of the numbers you provided. The fraud losses, were those all creditors in those examples?

MS. DESOTO: Yes. We're primarily talking about application fraud in the numbers I quoted although at the very beginning I talked about the $1 trillion loss for all of economic crime in the U.S.

MS. TWOHIG: Thank you. Moving along, Travis, could we hear from you next?

MR. PLUNKETT: Good morning everyone. My name is

Travis Plunkett. I'm the Legislative Director of the Consumer Federation of America. It's good to be here with you. I'm going to focus my remarks on the trend that you heard about towards increasing automation in the evaluation of credit histories and the credit score.

As of 1999, approximately 60 to 70 percent of all mortgages were underwritten using a credit score or automated evaluation of credit. More recent estimates by Fair Isaac indicate that 75 percent of mortgage lenders and over 90 percent of credit card lenders use this score in making credit decisions.

Now, you've heard about the good news. There has been increased speed in the granting of credit. There have been lower costs. And there certainly has been broader access by more Americans who 15 years ago couldn't have gotten access to this credit.

Now, as I'm a consumer advocate, let me tell you about some of the negative information. Then I'm going to provide you with data from our most recent report on credit scoring accuracy.

Of course, technology and information in automation are neutral. So the bad news is that this information has been used positively but also negatively. Some lenders have extended credit to sub-prime borrowers in an abusive and predatory manner, abusing their new technological capabilities to develop usurptiously high interest rates and fees carefully targeted at unwitting and vulnerable consumers through a number of strategies which I won’t talk about in detail here but we can talk about later. Upselling is one.

These lending practices contributed to an unprecedented growth in bad credit card and mortgage debt, home foreclosures which are at near record highs, and let me also mention the personal bankruptcy rate, which is at a record high.

Now, of course, automation isn’t the major factor in all of those problems but it certainly is a contributing factor. And, finally, accuracy. Accurate information is the foundation of this entire system of automation. I can't explain what is at stake better than Howard Beale, the director of the Bureau of Consumer Protection here at the FTC, has done it so I’m just going to quote him, quote, because even small differences in a consumer’s credit score can influence the cost or other terms of the credit offer or even make the difference between getting approved or denied, accuracy of information underlying the score calculation is paramount.

Now, the Consumer Federation of America and the National Credit Reporting Association looked at accuracy, completeness and differences in the score between the three major reporting agencies in December. As far as I know, this is the most exhaustive study of credit score accuracy and completeness that has ever been done. We looked at over 500,000 credit files. Every state and territory in the nation was represented.

Findings: nearly one out of three files, that’s about 29 percent, had a score discrepancy between the three major reporting agencies of 50 points or more. Now, as you may know, credit scores range from on the low end around 400, around 400 to on the high end around 800.

Four percent of the files we looked at had a discrepancy of more than a hundred points. Now, one of the issues about this finding that has been raised on Capital Hill is well, come on, that’s like the difference between say, Coke and Pepsi or the ACLU's take on one particular legislator versus the National Taxpayer Union’s score or rating. That just isn’t so. And you’ve heard why.

These scores purport to be predictive of consumer credit behavior. They purport to be objective. We shouldn’t be seeing variations between the three agencies even though the type of information they collect can vary. They have different strengths and weaknesses in the type of information they collect, we shouldn’t be seeing differences of this magnitude.

We looked at this information in three layers. I told you about the largest sample. In the next largest sample we looked at the impact in particular on mortgage borrowers on the bubble between lower cost prime credit and higher cost sub-prime credit. We found about 20 million vulnerable consumers around the 620 credit score level who, if their credit score was a little higher or a little lower, could be paying more or less.

Roughly 8 million, one in five of those who are at risk, are likely to be misclassified, according to what we found, as sub-prime upon applying for a mortgage based on our review of credit errors and inconsistencies.

A similar number, this is important, are likely to benefit from errors in the reports. However, I don't think anybody in this room is going to endorse the notion that the credit score should be kind of a lottery system. Consumers don’t benefit from systemwide averages. So we need to talk about specifically how to eliminate those variances and make the situation better so that more consumers are getting a more accurate score.

Finally, in our smallest sample we looked at why these errors were occurring. Were they errors of omission such as nonreporting of information or errors of commission, incorrect or inconsistent data included in the report? One of the bi15 8.y-aude h0.0001 Tc(report? One off-4.8bo information.

This is information, for instance, complete information on a consumer's positive credit history, their payment of their mortgage loan on time, the ratio of their balance on their credit card to the overall amount of credit that they have been offered. Huge problem there.

What we found was nearly eight in ten files were missing a revolving account in good standing. One of three files were missing a mortgage account that had never been late. Reporting on credit limits and balances, which anyone who has studied credit scoring will tell you is a significant factor in that score, that is how much do you have out versus how much have you been offered, reporting on that was almost universally inconsistent.

Let me mention that that particular finding is consistent with the findings of a Federal Reserve report out this February. In fact, one of their major findings was that reporting on limits and balances was not accurate.

What we have here is an automation problem. The default setting, so to speak, when they report your balance is your balance. So in many cases furnishers and creditors, aren't supplying the information on what your credit limit is. They're simply supplying the information on what you balance is and then the system defaults, in terms of your limit, to what that balance is. So if you have a balance of $500 and the system shows that your overall limit is $500. It shows you maxed out. And that is a ding on your credit report, on your credit score.

That's a summary of our report and the concerns. We can debate policy resolutions to these concerns. Just in closing let me mention that if the accuracy of credit score information is in question and the accuracy and completeness of the underlying information that is used for credit scoring is in question in significant cases for one price point, in this case we're talking about that 620 credit score, then as the credit industry moves more and more towards risk-based pricing it's going to be a concern for more price points.

For example, we learned recently that one insurer in Florida now has 50 -- that's right, 50 price points for their insurance product based on the credit score. So if we found problems around the 620 point, imagine 50 of those. I mean, at this point, given the research that we've done we're most concerned about that prime/sub-prime borderline.

For folks on the high end who have a 730 credit score or a 760 credit score, that variation doesn't matter as much. But as we go more and more to a risk-based pricing situation where you have a whole range of prices that are offered then those kinds of variations matter more. I will close with that point and then we can talk more about some of the other implications of this problem and other problems of misuse of credit scoring later on. Thank you.

MS. TWOHIG: Thank you, Travis. Evan?

MR. HENDRICKS: Thank you, Peggy. Thank you, FTC. I’m here to talk about the benefits to identity thieves of certain information flows and the costs and the damages to some consumers.

Thieves steal identities so they can take out credit in people's names. They're able to do that because when they apply for credit the credit bureau discloses the credit report of the innocent victim to the credit granter taking the application from the identity thief.

Now, why does this happen? It happens because the credit bureaus generally accept partial matches of identifying information so the Social Security number doesn’t have to be exact. Sometimes it can be a one or two digit difference. The last name doesn’t have to be the exact same thing.

This has been well exploited by identify thieves and when they do use the exact same Social Security number, which is what identity thieves usually do, then that can override all the other identifying data. The identity thief can be putting forward a different last name or be in a different state but if they have the same Social Security number, it will still spur the disclosure of the innocent victim's credit report.

Now, this partial match was also the cause of mixed files which was the leading cause of complaints to the FTC in the early 1990s. Now, identity theft, which is really a subset of mixed files, is the leading cause of complaints because in identity theft the thief's generated data is polluting your credit report.

When inaccuracies arise, the consumer dispute resolution process doesn't always work. Let's say you discover that your credit report shows you're nine days late on a credit card from the XYZ credit card company either because of identity theft or a mixed file.

You tell by writing or calling the credit bureau that you've never done business with the XYZ corporation but the process, they use an automated process where the credit bureau will send an automated message to the credit grantor saying, reducing your dispute to a two-digit code, usually meaning not mine. The consumer says not mine.

The credit grantor receives this code and then it looks to see if what you're disputing is what it reported before. And then it often says no or yes we did report them 90 days late before. So we confirm that. The credit bureau comes back and says we have verified the information.

In other words, this is an electronic version of did you say this and they said, yes, I said that. This does not really constitute a true investigation. Why do they do this? Well, because of the volume. The credit bureau disputes can run from 5- to 25,000 disputes per day, usually in the range of 7- to 10,000. A year and a half ago Capital One said it was getting a thousand disputes per day about credit reports. A year ago it was 2000, and now in the spring, it's getting 4000 disputes per day.

Clearly, the need to hold down personnel costs is particularly the Meth-Amphetamine users, or Tweakers as they are called. Others consist of foreign nationals, including Nigerians, Lithuanians, Russians, Asians, and Middle Easterners.

Others are made up of gay cross dressers with names like House of Con and House of Ebony. In the past seven months, postal inspectors have made 2264 identity theft related arrests from mail theft.

Thus the flow of financial marketing information containing consumers' personally identifiable information is facilitating identity theft.

Now, also, we have not really developed a formula for measuring or gauging these damages to consumers and so I would like to quickly run through this in about one minute.

These are some of the typical damages from being a victim of either identity theft or an inaccurate credit report. You can be inaccurately described as a dead beat and you are improperly denied credit. You expend time and energy to correct errors not of your making.

You wrongfully receive debt collection calls. You're chilled from applying for credit. You have physical symptoms. Your sense of helplessness, loss of control of your personal information and the emotional distress stemming from all of the above.

I clearly believe these are damages and costs to consumers and if someone doesn’t I would be curious to hear why. So we need a formula and maybe Fair Isaac can donate pro bono some of its skill as statistician to assign

Abernathy, who will be here later today, used the term one million. We don't really know exactly how many victims of identity theft. We do know that the number is doubling every year.

Now, also, Travis already touched on this the industry is saying they're worried that privacy will restrict the free flow of information. In fact, credit grantors trying to game the system, trying to hold onto their own best customers by not reporting their credit limits is really the main obstacle to the free flow of information and they're doing this voluntarily.

The June 12th American Banker reported Capital One purposely does not report consumers' credit limits for competitive reasons. Then they make people look like they're maxed out, lowering their credit scores. I don't know how many customers Capital One has. I know it runs in the millions.

In closing, I would like to show a very quick video because ultimately the argument is being made that privacy protection is bad for the economy. Can we run this video now so we can see a quick rendition of how this argument can play out?

MR. HENDRICKS: By Citizens for North Dakota's Future which ran in advance of the referendum on the opt in financial privacy law.

(Whereupon, a videotape was played.)

MR. HENDRICKS: The argument was made that it was bad for the economy. The argument was rejected by 72 percent of the voters. I think they saw through it as shallow. Since the referendum, by the way, one bank has expanded its call center and created more jobs and another bank has opened a new call center in North Dakota. I think that you should look at the statements of Joel Reidenberg and Julie Brill before the House that the states with the best privacy protections, Vermont and Massachusetts, have the lowest bankruptcy rates and the best interest rates.

California, which also has good privacy laws, also is better than the median when it comes to bankruptcies and has a good mortgage interest rate.

I think that the argument that privacy law is bad for the economy is suspect and any studies purporting to say that should be looked at closely. Thank you very much.

MS. TWOHIG: Thank you, Evan. Well, I think we have a considerable challenge ahead of us because as you can see there is all kinds of different information that is used in making credit transactions, and one of the challenges in just discussing this issue in the remaining time we have is that there is various stages to the credit transaction.

You heard some of the issues mentioned with respect to each. There is the basic marketing stage, getting the consumer in the door or online or on the phone. Then there’s the decision stage which involves making sure the financial institution knows they’re dealing with who they say they are dealing with, that the person is who they say they are as well as deciding whether they're going to do business with a person in terms of underwriting and on what terms.

And then, of course, it even goes from there in terms of account review and management and further marketing cross-selling. Given that challenge I think what I’d like to do to try to home in a little bit on the costs and benefits and specific data and specific examples is to break it down and let’s talk first a little bit about marketing in particular.

Something I would like maybe Pete to start addressing is how important is it that the marketing that is done and what are the benefits to business of using personally identifiable information? By that I mean the marketing that is done perhaps using the prescreened database from the credit bureaus or other personally identifiable information as compared to more aggregate data which presumably has less privacy concerns.

MR. MCCORKELL: Well, personally identifiable information is important because it helps us understand whether this person is a good prospect. Somebody that already has a half a dozen credit cards is probably not a very good prospect for us, and you can't get that at the ZIP code level.

It understands who's a good risk. It's much more effective to be able to go out with an offer of credit than with a solicitation, well, please send us an application and we'll consider it.

Maybe the best indicator of the effect that credit bureau prescreening has had on the economy is to compare interest rates on credit cards today to what they were, say, 25 years ago before there was prescreening. Twenty-five years ago, regardless of what the prime rate was doing, 18-percent was a spectacularly good interest rate on a credit card and a lot of them were 21, 23 percent.

There was very little national competition. If you wanted a credit card you went to your bank and hoped that they issued it. If they issued it, maybe you went to another bank and maybe you got one and maybe you didn't.

Today the market for credit cards is essentially nationwide as is the market for mortgages. That competition factor, again, makes us act more efficiently in terms of who we market to, at the same time it makes the cost of credit much more affordable and much more available to a larger segment of the population.

MS. TWOHIG: Evan or Travis, do you want to comment on the cost to consumers on the flip side of the personally identifiable marketing and in particular the prescreening process?

MR. PLUNKETT: I wouldn’t deny that prescreening allows better targeting. I think most experts though would dispute the notion that the main reason for the drop in credit card interest rates is this trend. The main reason for the drop in credit card interest rates since the late '70s and early '80s is the drop in the cost of capital.

I mean, just in the last three years the benchmark rate has dropped significantly and when the Fed puts out its report at just about this time every June that is the main reason that they cite for a drop in interest rates.

MS. TWOHIG: Evan?

MR. HENDRICKS: I also agree that for many years prescreening played an important role in expanding credit and it was beneficial to consumers in many ways. But time evolves and circumstances evolve and I think that given the fact that credit is so plentiful and there are so many ways to get credit and the fact that now we know that identity thieves are looking for financial instruments, we have to rethink how much strengthening consumers need in their right to be able to not receive those sort of offers.

MS. TWOHIG: It also seems to me that one of the costs of allowing creditors to access the credit database to do marketing has also been there have been reported problems in creditors then pulling back. I think that’s been alluded to and not reporting complete information in order to protect their best customers. Does anyone want to comment on that situation as a cost of prescreening or what the data shows there?

MS. DESOTO: Sure, I’ll take that one. First of all, I think it’s absolutely foundational to a national credit reporting system the concepts of quality and accuracy and completeness. So from the perspective of a credit reporting agency we actually look at quality in five different dimensions. So we definitely look at completeness or content, depth, accuracy, currency and consistency. So that's foundational to the system.

As was mentioned earlier this morning, we do have a voluntary system of reporting, and certainly Experian, and I think I speak on behalf of the entire industry, is a strong supporter of full file data reporting by all lenders.

Certainly we want to go on the record for saying that, and we take many proactive measures to go out and seek lenders who are not currently reporting to the system.

I think in that sense we are absolutely in agreement with the comments made earlier today that the whole system is strengthened by full file data reporting and completeness of the data.

MR. HENDRICKS: And that's a widespread problem, Laura, in creditors not reporting?

MS. DESOTO: I wouldn’t say it’s a widespread problem. As I mentioned, we do have efforts on an ongoing basis to reach out to credit grantors and many times they are smaller organizations who need prodding or some expertise in understanding how do I even report to a credit reporting agency. Give me some support. Give me some advice on how to do that, and those are active efforts.

MR. PLUNKETT: On that point I’d like to quote the Controller of the Currency as to his assessment of the cost. Sub-prime loans can become a vehicle for upward mobility of creditors in the broader credit market, lack access to consumer credit history, yet a growing number of sub-prime lenders have adopted a policy of refusing to report credit line and loan payment information to credit bureaus without letting borrowers know about it. Some make no bones about their motives. Good customers that pay sub-prime rates are too valuable to lose to their competitors. Now, the cost there to the consumer is obvious. They’re stuck in a higher rate, higher cost loan.

Another issue that doesn’t involve prescreening but relates to marketing has been raised in a lawsuit by the organization Acorn against Household Finance, filed in 2002. Household Finance obtained a list of clients from affiliate retailers including Best Buy, K-Mart, Costco and a few others.

Homeowners with high rate credit card and other consumer debts were identified from these lists and

In other words, full file reporting; there’s not enough information in the file or consumers don’t have enough information or not identifying the person accurately which you can only do with more information to identify them.

It seems like in many ways the issues or the problems identified with credit reporting really would argue for legislation requiring more information flows. Instead of looking at ways to restrict information flows, the way to make a credit file more accurate is to ensure that there’s greater access to information and that access is guaranteed by law, that there are ways to verify that information and that it is the absence of sufficient information flow that’s really at the heart of many of the problems, many of which are well documented. I’m not in any way disputing the existence of the problems. I’m wondering how if you can possibly solve those problems without greater --

MS. TWOHIG: If I could just ask Fred one question. How do you see the ability to use the credit bureau database for marketing purposes as relating to the current situation of incompleteness of data?

T c (1) T j / T T 2 i

an individual’s actual information rather than accurate or predictive or guessing if you will.

Therefore, to the extent that you either make that data less available as a matter of law to use or you make it more expensive to use or you create incentives for providers of that data, particularly creditors, not to provide it, whether those incentives are cost or regulatory or whatever, you inevitably come back to make either less information available or you run into the accuracy problem.

MR. PLUNKETT: I’m going to agree with him here on this point. We’ve crossed the line between marketing here and underwriting, and from the consumer point of view we make a real significant distinction. On marketing we think consumers should control the secondary uses of information for marketing purposes but to go to the question of underwriting, absolutely, what we proposed is that if a furnisher, a creditor, for example, uses the credit reporting system they should report completely.

We would agree that more information in the situation of underwriting is a good thing. Now, that’s not a mandate. That’s if you use the system, use it right.

MR. HENDRICKS: It’s a standard. It’s still going to be voluntary but if you report the standard is you have to report completely.

MS. TWOHIG: And Travis, since we are moving to the underwriting issues where accuracy is critical, if I could just ask you on some of what your report talks about. It seems to me there is a difference between accuracy and completeness and one, perhaps, cost of our voluntary system is that in some sense you're never going to have exactly identical data in every credit bureau as opposed to, perhaps, if you had a system that it was required and it was all lock step, exactly the same you would probably still have some accuracy issues just from volume of data. Could you say a little bit about that?

MR. PLUNKETT: Sure. It’s a good question. Well, we don’t have a command and control system. We don’t have one databank. We don’t have a Soviet-style credit reporting system so we are going to see variances. But we’re talking about the increased use of the credit score in automation where you take that underlying data and you come up with a predictive factor. If the end product isn’t effective then I guess my response would be there are going to be some variances between the three agencies but that end product, that score, we shouldn’t be seeing the variances that we’re seeing because that is what’s used by lenders, for example, to grant credit or to not grant credit or to grant credit at a particular rate or under certain terms.

So whatever the underlying data we shouldn’t be seeing variances like we're seeing with the credit score given that so many lenders now just look at the score.

MS. TWOHIG: Anyone want to respond to that?

MS. FIKE: If I could comment briefly on that. I think I hear Travis questioning whether using a statistical based system to help assist in the credit underwriting process is legitimate or not. Fundamentally the question that any creditor has to answer is whether or not to extend this credit to this consumer. Is that going to keep me, A, competitive in the marketplace and if I give this credit on these terms and if I do will it be accepted. And B, if I give credit on these terms, will I have losses that are going to cause me to end up out of business.

You can make those decisions on a spectrum from pure judgmental systems like we used to have before scoring assisted or with a combination or using automated systems.

Fundamentally, you're pointing to differences that you have identified in the results of the scoring system which are driven in many cases by simple differences in data, not necessarily inaccuracies in data but in some cases pure timing differences and therefore suggesting that the system is somewhat flawed. I guess I take issue with that.

I, however, believe your study is important in that it helps educate consumers about the fact that there can be differences. We believe that consumers should understand how credit scoring works and we want them to understand that. We want them to see how lenders see them. We encourage consumers to check their scores at all three bureaus and we encourage them to check their score before they undertake a major purchase like a mortgage or car financing.

So while the point is valid that people should understand how these systems work, I'm not sure that the fact that there are temporal differences implicates the validity of the system.

MR. PLUNKETT: I just would respond on one point. Temporal differences don't account for what we found. We looked at, for instance. The issue of loading data at different times by the three credit reporting agencies. It's in our report, those differences do not account for the variances that we found.

The other issue I'll raise is that if we did have more complete reporting then hopefully we wouldn't see the kind of variances. And, you know, whether there's an error or a lack of complete information it's kind of a distinction without a difference to the consumer if their credit score is 610 and it should be 670. Either way, they're going to face higher costs and maybe not get credit.

MS. TWOHIG: Evan?

MR. HENDRICKS: Well, I’m glad Fair Isaac does want people to see their credit scores now because it didn’t always used to be that way. So it is better now that people are able to see it. I remember Chris Larson at e-loan almost got suspended from access to credit reports because he insisted on giving people their credit scores.

But public pressure plays a very important role in this which is why I wanted to ask Andrea, let’s say you’ve got a consumer who’s satisfied with his credit, likes the number of credit cards he has, and basically, wants to opt out from prescreening. And he opts out from prescreening.

Don’t you think that should make the credit score go up? If you say I don’t need any more credit card offers. I’m very comfortable with where I am and I’m not going to be tempted by offers and hey, I’m where I want to be, doesn’t that show a responsible consumer? Shouldn’t that make their credit score go up?

MS. FIKE: Since I’m not one of our scientists I’m not sure I could really answer that question. I guess we have to look at a statistically significant sample size and see whether or not that has a legitimate correlation.

MR. HENDRICKS: I would be concerned, though, that your industry doesn’t want people to opt out from

more about that?

MR. MCCORKELL: Yes. As I pointed out there's a very real difference between the information that's in the system of record about any particular credit product with detailed transaction data, the fact that you spent $50 at Amazon and $40 at the pharmacy and that very detailed data that I think is the source of a lot of the fears on this versus the customer information system that tends to be much more summary data.

It may have the fact that I have a credit card. It may have the fact that my limit is X and I've had the card since such and such a date, that my current balance is Y, that I've never been delinquent. But it's not going to have that detailed transaction data.

As a practical matter, regardless of the legal situation, constructing a customer information system that had all of that detailed transaction data is a gargantuan and maybe close to impossible feat to pull off correctly.

One of the things that I've seen really over the last 10 or 12 years were financial institutions that tried to construct customer information systems to bring all those information relationships together.

A lot of the early attempts failed because people didn't put any limits on what they put into that centralized database. They had too much, it became a

and I don't think most financial institutions are trying to do that any more because of the customer reaction and because of the technical infeasibility of doing it.

MS. TWOHIG: But to the extent you can you are using it for cross-selling and also at the decision stage?

MR. MCCORKELL: Well, again, we’re not using that individual transaction data very much at the cross-selling or decision stage. We’re using the account level of data in the customer information field. To the extent we are dealing with third parties, even that is probably getting filtered once again through a marketing database so that we provide really the minimal information we need for third party use. In our case probably close to 90 percent of that is involved in insurance sales for very, very accurate organization.

MS. TWOHIG: Evan or Travis, did you want to say anything about affiliate sharing and the potential cost to consumers on that issue?

MR. HENDRICKS: The main issue with affiliate sharing is that affiliates often represent different purposes and the consumer doesn't expect information collected for a checking account to be used to sell them securities.

The other issue coming up is that a study, we keep waiting for it to come out from Michigan State, saying

though I think we could go on talking about these issues all day. I want to thank the panelists for their excellent presentations and also an interesting discussion.

(Whereupon, a lunch recess was taken.)

against fraud deception, security for their data, and privacy.

We recognize that there are lots of people involved in giving consumers those tools including government and businesses and even consumers themselves. Now, this afternoon, and for that matter for this whole day, we have talked a lot about how we measure the costs and benefits of the collection and use of consumer information.

But what I would also say is that we need to be sure that we capture the true costs and benefits to consumers. Th we d between marketing and consumer confidence and we'll hear a little bit about what industry and others are doing to measure the consumer experience and how business develops their face to the world.

I also think it's an opportunity for the panelists to tell us how they include consumers in their own values proposition. So it's an interesting panel and I look forward to hearing your presentations. Thank you very much for being here today.

(Applause.)

MS. OHLHAUSEN: Thank you very much, Commissioner Thompson. Welcome to the panel on customer relationship management, which is also called CRM for short, and targeted marketing. I'm Maureen Ohlhausen. I'm the Assistant Director for Policy Planning here at the Federal Trade Commission.

We will first start off with remarks by each of our panelists and then we'll have a discussion so I'd like to first introduce our panelists.

We have Marty Abrams Executive Director for the Center for information Policy Leadership; Dave Schrader, Lead Strategist and Marketing Director for Teradata; Nelle Schantz, Program Director for CRM Solutions at SAS Institute; Sandy Hughes, Global Privacy Executive, Proctor & Gamble Company; Rick Savard, Senior Vice President, Marketing Services for FACS Group.

Then we've had a slight change in the order. Next we have Beth Givens, Director of the Privacy Rights Clearinghouse and batting cleanup we have Larry Ponemon,

the marketplace. They're things like fulfillment, customer service, risk management, product development, which is to me the most important, sales and marketing.

So what we're doing is applying the technologies of CRM to all of those traditional applications. What is different about CRM and is really the concept of centralized information management. It's either that you have a data warehouse or you have good ways of linking data that are distributed together to come up with a 360 degree view of the consumer.

All the data is accessible for all of the applications so that you understand the best way to service that consumer. So what has really changed is this concept of bringing all the data together. In the old days when I first started at TRW systems, the company did one thing and one thing well. So you had all the data in one system together. Today, we have a common place for the data and we have multiple processes running off of that common data system.

Let me give you some practical examples from the marketplace. I still think we're very new into the CRM marketplace. I think probably where CRM has been best applied is in financial services. But let me give you some concrete examples of how you change the market when you begin to have a 360 degree view of the consumer.

One organization I knew had 400 data platforms because they were built through many, many acquisitions. They knew that they had 80 million distinct customers in those 400 data platforms. They knew it was not possible that they actually had 80 million customers, but they didn’t know how many customers they actually had until the consolidated down to one data system or one data platform.

At that point they could begin to deal with those customers and do things like preference management that they could not do before they had consolidated down to one data system.

Another organization, a direct marketer for a customers, sent them a lot fewer catalogs, became a lot less of a costumer for people’s parties. So they began to understand better who their most profitable customers were.

We already had the mention of Amazon this morning that analyzes your purchasing behavior so that they can begin to model what type of products you might want to buy tomorrow, what type of books might be available. They are an example of an organization that has used information to model behavior.

Lastly, we have an airline that began to match their complaint data with their data on frequent fliers. They stopped sending their frequent fliers who missed big meetings and sent complaint letters with congratulatory messages about how wonderful a job they were doing online arrivals, cut down the angst level of those particular travelers. Simple concept that happened when you begin to integrate data together.

When we think about these questions all of these applications have trade-offs for consumers. If I’m the consumer who has been renting for free these clothes from this particular cataloger, I lose the ability to be able to game the system.

I game a particular airline. They think that I start all of my trips in Washington on a Friday, go back to Dallas, spend the weekend in Dallas and come back to

include unsolicited commercial e-mails, often called spam, irrelevant banner ads and even unsolicited paper mail or junk mail.

Bad marketing people use and abuse these channels by sending out too many marketing messages to too many consumers. Recent statistics show that a typical American this year will receive more than 2600 unsolicited e-mails, will see roughly 8900 banner ads and will receive more than 34 pounds of third-class mail.

As a result, consumers are becoming annoyed and even clamoring to outlaw unwanted communications. But it is important to understand that most responsible companies want to behave responsibly so that they can create and build enduring customer relationships.

Good companies realize that every consumer creates numerous clues about what he or she wants and these come in the form of purchases, browsing behaviors on the web, interactions with call center agents and even e-mails. It’s a balancing act to collect this information without intruding on privacy.

But, when it is allowed by consumers, good marketing companies capture these clues in data warehouses and use analytical techniques like propensity modeling to determine what products might actually be a good match for each customer. They realize that not all products are relevant to all customers at all times so they create small customer segments and try to provide individualized offers and personalized customer service.

For consumers this is exactly like going back to the pre-computer days when the merchant might greet you by name when you come in the store, remember what you bought at a last visit and highlight newly arrived merchandise that you might like. That’s the primary use of consumer information, to delight each customer with a great experience.

Now, the way one can distinguish between good and bad marketing is to take a look at two measures. Conversion rates, defined as the percentage of people who respond to an offer, and customer satisfaction rates, either measured on a one to ten point scale or by metrics like return shopping behavior.

Bad marketing people who spam get very, very low rates. One recent example cited only 36 responses to 10 million e-mails for an herbal supplement which translates into a 0.00036 percent response which is very, very poor. Only 36 people out of 10 million.

By contrast, I’d like to show you an example of great marketing by one of our customers. It's a large international bank. Every day their Teradata data warehouse system looks through all the banking activity by their customers for significant individual events such as an out-of-bounds or large deposit or withdrawal, gaps between the original loan rate they got and the current rates which may have dropped, and events like CDs coming due.

Every night 370 analytical programs called event detectives look for these clues. The system generates 42,000 leads per week which are then evaluated and handed to personal bankers who do follow-ups via phone or e-mail at a time chosen by the consumer.

This high touch, relevant approach to banking has paid dramatic dividends. By basing the marketing activities on consumer behavior the bank has seen responses to its campaigns of up to 60 percent. Average customer conversion rates are five times as high as before doing this kind of event-based marketing.

Customers like the approach so much that they deposited an additional $2 billion with the bank within the first six months of the program.

Finally, because event-based marketing works so well, the bank decided to stop doing most mass mailings. As a consequence they were able to chop 75 percent from their advertising budget and they have saved $20 million in postage costs.

This bank is not unique. Numerous customers of

Teradata are reporting similar numbers when they adopt event-based marketing programs. The three steps include one, detecting key events at the individual customer level; two, responding with an appropriate offer personalized to that customer; and three, measuring the results to know what offers work and which don’t thereby continuously improving the ability of the bank to please its customers.

Good marketing pays off with conversion rates in the 25 to 60 percent ranges as well as much higher customer satisfaction numbers.

Across the industry we’re beginning to see numerous statistics that show the profound difference between marketing people who collect the clues and analyze them and those who don't. This chart shows that good marketing practices can be 11 to 63 times more effective than bad ones.

For example, only one in 300 people, 0.3 percent, will click through on a banner ad if it’s not targeted correctly while one in five people, or 21 percent, will respond if it is well matched to their needs. Similarly, companies who do a good job of targeting their physical mail offers can see a 36 times difference in their effectiveness by using analytics. The final line of the chart shows the difference in customer satisfaction, a factor of 30 when it comes to repeat buying rates.

In summary, using analytics technologies like the ones Teradata offers can make a huge difference between bad and good marketing. It is a win-win situation because the company usually spends less money on marketing for a higher return. The consumer benefits, too, because she will receive fewer but more relevant messages which cause higher conversion rates and higher customer satisfaction. Thank you.

MS. OHLHAUSEN: Thank you very much, Dave. Now we have Nelle Schantz from SAS Institute.

MS. SCHANTZ: Thanks, Maureen. Let me begin by saying thank you and thank you to the Federal Trade Commission for sponsoring a workshop where we can sit here and discuss data and discuss facts about how to use customer information.

I appreciate the opportunity to add insight into the discussion on this panel today. Let me begin by pointing out that I work for a company, SAS Institute, that provides software to companies to gain or acquire better insight about their customers and to improve their customer relationship management strategies that Marty went through very well.

We maintain the position that leveraging customer information, if used responsibly, is beneficial not only to the company but also to consumers. So what I’m going to do

satisfaction data, pulling in information like that to get as complete a view of your customer as you possibly can.

The second step is as you're pulling that information in is cleansing it, making it more accurate. You want to be able to as we heard from Acxiom this morning do things like make sure that Jane Brown's data is combined with Jane M. Brown's data.

What we found is that these first two steps are the foundation for creating good relevant insight. SAS just conducted a survey in Europe. We surveyed and interviewed 500 marketing directors in financial services institutions and telecom institutions.

Sixty-seven percent of those companies said that inaccurate data and incomplete data was having a negative impact on their profitability of the company. And consequently, it was also having a negative impact on the customer satisfaction and the customer loyalty.

So getting this more complete view of a customer, getting this more accurate view of a customer is a foundation that you've got to have in order to start using the analytics that I'll get into now to create that customer insight.

The third step here is the analytics piece, using analytic technology to analyze your data. What companies are doing with that is they can start off as basic as doing reporting and looking at historical data and trends to getting more sophisticated, using what we call data mining or predictive modeling.

That is technology that gives companies the ability to get their arms around huge amounts of data and to gain insight from that data using statistical models and predictive models.

It's that type of process that helps companies answer questions like who is in danger of leaving my company or what is the next best product that this customer is going to be interested in that I should talk to them about. Or, maybe on the flip side, who is a potential money launderer in this company?

So it's the predictive modeling and the data mining that is going to give you insight like that. Once obtained, you want to take that insight and have technology that helps you deliver it or deploy it into the front office channels and into the hands of the employees that need to use that data to have more effective interactions with their customers.

Just a summary, the four steps are accessing data, cleansing the data, performing analytics to create your customer insight and then delivering that insight out to the people that need to use it or the system that needs to use it.

Let me switch gears and give you a couple of examples about why using this type of technology and these practices, again, when used responsibly, can benefit the customer. We've got a lot of examples, from the companies that we work with of how companies will identify profitable analytics to identify customers that were unprofitable.

They sent a note to those customers which said, thanks for being a customer. We are going to start charging you're a $25 annual user's fee because they wanted to make it more profitable.

Well, consequently, a lot of customers ended up closing out their credit card account and at first they thought that was fine because it was improving the profitability of their credit card portfolio. But what the bank came to find out was because they did not have a complete view of their customers and weren't looking at a well rounded view what they ultimately found out and determined was that the least profitable credit card customer was the most profitable banking customer.

So they also lost mortgages, savings accounts, deposit accounts, and investments. That's a great example as I'm wrapping up here to share with you maybe a best practice learning from that and that is that companies in implementing CRM solutions or implementing CRM strategies are not focused just on technology.

They are driving at this from a best practices perspective. They are driving at this with a focus of delighting customers and retaining customers. Companies that are successful in this not only align their technology with that strategy but they are aligning their employee training, they’re aligning their center plans, they are aligning their whole culture to focus on delighting the customer. Thank you.

MS. OHLHAUSEN: Thank you very much, Nelle. Marty gave us the overview and Dave and Nelle both gave us sort of the general view of how these processes work. Now, I’d like to turn to some specifics and Sandy and then Rick will discuss how their companies in particular use this data and these kind of processes in their own operations. So, Sandy?

MS. HUGHES: Thank you, Maureen. I’m Sandy Hughes, Globicksn. I’m Sandy

customer. Thaksn. I’m Sandy

customer. Thaksn. I’m Sandy

gave us the ovksn. I’m Sandy

of the generalksn. I’m Sandy51 TrelTc(

like to turn tksn. I’m Sandy

discuss how thksn. I’m Sandy

MS. HUGH

transparency and trust. We offer individuals who provide us their information on choices, on how they'd like to get to the sites that way. It's also in our typical print ads and things we'll also put websites on there.

MS. OHLHAUSEN: Thank you very much. Rick?

MR. SAVARD: Well, I, too, will take advantage as Marty did to say thank you to the FTC. Thank you, Maureen, for the opportunity to participate in this important forum.

For those of you who may not know F A C S or FACS stands for Financial and Credit Services. We are the

Federated.

Let me give you two examples of how you can maybe gauge relationship equity. The first one is if when you conduct a customer survey you experience a response rate of 20 percent or above then chances are you probably have pretty strong relationship equity.

If you have a large percentage of your customer base that has been transacting and doing business with you over a long period of time, so these are tenured customers, let’s say ten or 15 years, and they have transacted with you each and every year chances are you have a high degree of relationship equity.

Customer data. First, regarding the control of data. I think we all agree that customer data is a very valuable asset. Consequently, you need internal system support to manage the data as well atel as qo TD0ncfo5n2/F1 1 TDnnT

8 cost, regarding thcusto 1e-/er da,is i, yos aof
9

Developing a customer loyalty program based on consumer behaviors versus spending levels. Historically, loyalty programs were designed based on the simple requirement of what you spent.

It was assumed that all customers who spent a predetermined amount of money with you, let's say $500, looked alike. Today, with the benefit of data sharing, our perspective on this topic is much more evolved.

Listed behind me on the chart is just a sample of the data elements that we would consider today when attempting to develop a customer loyalty program. What customers buy, the specific merchandise, the frequency of their visits, as well as when they visit, lifestyle data.

Do they use your store card or do they use another payment method, full versus sale price, the number of relationships that you have with that particular customer, do they revolve when they use your card, use of promotions, demographic data, do they take advantage of deferred payments, brands purchased and families of business that they shop. This is but a fraction of the data elements that we factor into decisions on how to tailor products and offerings to customers.

Well, the implications are pretty obvious. All customers that spend $500 with you are not alike. Unique customer behaviors are what drive enhanced customer satisfaction and profitability.

Lastly, this higher degree of success, in turn, allows companies to develop and deliver more relevant, compelling offers that, in turn, nurture stronger customer relationships.

Example number two, this is a little more of a challenging example in that what we are looking at here is the management of the entire customer life cycle. For many of us as retailers the motivation in our business goes far beyond the transaction. It really talks to the entire life cycle.

For some of us, for example, in the department store business, that life cycle truly is a lifetime. The richer the data we have as a customer progresses through the phases of their life cycle the better we can manage and respond to a customer’s needs.

The value of sharing data. Benefits to the customer. Let's look at why the value of sharing data is a win-win proposition. Better products that address their individual and evolving needs. Again, Marty talked a little bit earlier about how in the old days back in.

MR. SAVARD: West Philadelphia. That retailer was able to cater to the individual needs of the customer. The landscape today is about millions of customers. In the case of Federated it’s about tens of millions of customers that transact with us every year.

We see it just as relevant our ability to cater to their individual needs on a one-to-one basis as it was in yesteryear. But at the end of the day, it comes down to the data.

The second advantage is a greater value at lower

years ago our data was 60 days old. It was hard to get at and it was incomplete. Today our data is days old. We can access it in a minute and I can mobilize it the very next day.

More sophisticated safeguards and control of data. I won’t expand on that. Clearer communication with your customer, prospective customer of how the data will be used. I think we’ve touched on that.

And lastly, greater appreciation for the concept of relationship equity. For individual retailers their respective definition of relationship equity will become essential for them to understand in the future. Thank you.

MS. OHLHAUSEN: Thank you very much, Rick. Turning back now to some more general issues that I also think Sandy and Rick both touched on but I think that we’ll get into more, we have Beth Givens.

MS. GIVENS: Thank you very much. I appreciate the opportunity of participating on this panel. The title of my presentation is “What’s Missing From This Picture?”

We’ve heard several presentations from industry representatives today touting the benefits of the collection and use of customer information. These include the benefits of convenience and also of saving money.

I want to focus, in contrast, on two themes. First, there are significant costs to individuals and to society of not protecting privacy, and second, not all costs can be expressed in monetary terms.

And I think Commissioner Thompson expressed this well in his opening comments. I would recommend to the Federal Trade Commission that an important area of research for the FTC would be to come up with ways to determine the costs of not protecting privacy and also some of these intangible and nonmonetary costs to society as a whole.

MS. GIVENS: Privacy Rights Clearinghouse is a nonprofit consumer advocacy and research and education program. We're based in San Diego, California. We have been in existence since 1992.

For the past 11 years my staff and I have invited consumers' complaints and questions about a wide variety of information on privacy issues. From the very first calls that we started receiving in 1992 we observed that control is a critical issue for individuals, and it is the lack of control over what is done with their personal information that literally drives them crazy.

In the early days the majority of our calls were about unsolicited mail and telemarketing. By the mid-'90s that subject was replaced resoundingly by identity theft as the number one topic. And today we have a mix of issues, telemarketing, identity theft, credit and financial issues, Internet privacy and employment background checks.

People who have contacted us explain how their personal information, and it might be in the hands of another person, it may be a company, it may be a government agency, has in one way or another caused them harm, aggravation or fear.

I submit that a great deal of these strong feelings about privacy stem from the fact that deception and a lack of transparency undergird the collection and use of a significant amount of consumer information.

Let me use just one example, that being the so-called product registration forms also called warranty cards. These are often packaged with consumer electronics products and I’m sure you’ve seen them. In addition to asking for information about that purchase they also gather demographic information such as income, age, education, hobbies, home ownership and the like.

But actually one’s receipt is all that is needed to activate the warranty and demographic data certainly has nothing to do with registering the product. Indeed, the deception goes further. The address that the post card is mailed to is not to the manufacturer of the product but rather to a post office box of an aggregation company that compiles and sells this personally identified data to marketers.

Yes, most if not all of these forms have opt-out statements but they are at the end, very tiny, written in vague language and I have yet to meet an individual who's actually nottsaurn in

Many financial companies sell or share name, address, phone numbers, account balance, account types and account numbers with telemarketing companies.

Telemarketers in turn pitch products of dubious value, in my opinion, to those bank and credit card customers such as travel, entertainment and shopping clubs, also insurance policies.

Several major U.S. financial companies have been sued by state attorneys general in the past four or five years for their unfair and deceptive marketing practices involving the sharing and the selling of customer data. These include U.S. Bancorp, Citigroup, Chase, Fleet Mortgage, First USA and NationsBank.

What are some of these fraudulent and unethical practices regarding customers' financial data and the sharing of that data? One practice is called preacquired account telemarketing fraud where products and services are charged against the individuals' accounts without their consent. This is achievable because the financial company shares that account number with the telemarketer.

U.S. Bancorp, Minnesota Attorney General is one of those cases. Now under Gramm-Leach-Bliley you cannot sell the account number but it is encrypted and actually the end result is still the same, that account can be debited.

In a 2001 case the Federal Trade Commission v. Citigroup a former Citi financial employee explained in a sworn declaration that branch managers targeted deceptive loans to individuals who they identified as vulnerable because of being, quote, uneducated, inarticulate, a minority or particularly old or young, end of quote.

Travis Plunkett this morning talked to you about the NationsBank, NationsSecurities case where affiliate sharing resulted in a lot of people moving into riskier investments and losing a considerable portion of their life savings.

Now, I mentioned at the outset that I would talk about the cost to individuals and society of not protecting privacy. Certainly these fraudulent and unethical practices that I have just described have very real and significant costs to many individuals.

This coming summer we're going to see the launch of the Federal Trade Commission’s national do-not-call registry. It’s been a long time in coming, and I, of course, speak as a privacy and consumer advocate when I say that, and I d c act1 Trit t2 1k9laythat Ihe Ftryog proltieallsumportiformthis megistry. isIhe Fesulteof theisTj/F1 1 Tf telemarketing calls every day. And this is even during a time when targeting has presumably been improving.

What are some of the costs to consumers? Well, the expense of phone services such as unlisted numbers, caller ID, anonymous call rejection, privacy manager, answering machines, voice mail services and devices like Telezapper, the Phone Butler and EZ Hangup.

I want to say just a few words about identity theft. Certainly this crime is testament to the negative addresses out of the hands of their batterers and stalkers.

You don’t often think of one's address as being highly sensitive but it certainly is to a victim of one of these crimes. The same holds true for people in certain occupations like law enforcement, court officials, teachers, doctors, social workers, celebrities, political leaders.

I encourage those of you who are designing CRM and target marketing systems to keep the needs of these individuals in mind as you design your systems because I think if you can serve them and still give them the benefits that you profess that you also will be helping others as well.

covering.

One is a very good report by Robert Gellman called “Privacy, Consumers and Costs,” and it does get into a lot of these costs that are not thought of when you don’t protect privacy.

Secondly, is the EPICs comments the Electronic Privacy Information Center that are out on the table out there and they offer a method for evaluating the cost of information flows.

Third is something that I wrote two years ago called “The Information Marketplace” presented as comments to a Federal Trade Commission workshop on that subject. And I get into a lot more discussion of some of the deceptive practices of collecting consumer data.

So again, I want to thank you and by the way, in answer to Commissioner Swindle’s earlier exhortation to show him the data, all of these papers have very good footnotes and a lot of well cited data and legal references. Thank you very much.

MS. OHLHAUSEN: Thank you very much, Beth. We now have Larry Ponemon.

MR. PONEMON: Thank you for allowing me to be the cleanup person. It’s kind of a deja vu experience. I feel like I was just here. I was. What I’m going to do is maybe spend about eight minutes to go through some data that I’m going to report upon. This was research that was recently conducted. I’m just going to give you a high level cut. If you want more detail please contact me. Many of you have and I appreciate the phone calls that are stuff. Keep in mind that if you're an organization and you are not walking the walk that is probably just going to just devastate your CRM efforts even if you have a good policy and even if you really have great interaction with your end customer.

So what are some of the key assertions about the privacy management process? Well, we all believe that a good process helps to reduce cost. We tend to measure cost like a compliance thing that if we do it right we're not going to get sued as much.

Well, it is also about making policies real and educating employees and other stakeholders. It's also a tool, a process and a tool, that helps provide feedback because we make mistakes. Most privacy abuses are ones we never read about because they're just not that interesting; they are about people making mistakes like sharing data and not really understanding that it's a violation of the law.

Now, the big assertion that is still untested is the idea that if you align the perceptions and beliefs of customers and targets, consumers, you will increase the confidence, their confidence in your organization and that will translate into new revenue. We all see that, that connection is clear to us but it may not be something that we can test or test very easily.

Now what are companies doing today? I'm not going to go through this. If you're interested we just completed a benchmark study. But in drawing upon the 150 or so items of the study I just pulled out a few interesting items to show you what leading companies, 55 leading companies, are doing today to build more of that value proposition on the trust side.

Number one, only 15 percent of the companies are actually linking privacy to their ROI framework, which I will discuss hopefully a little bit later, is a mistake. It needs to be linked.

Fifty-three percent of companies are actually attempting to capture consumer privacy preferences in their systems. Thirty-four percent are actually doing a double check to make sure that the choice that a consumer or customer makes is being honored. That can be dangerous. Fifty-eight percent actually attempt to align the policy with the expectation of the stakeholder.

Eighty-three percent have a process for communicating the policy. Forty percent have an outreach program to new customers. Forty-eight percent believe that they have sufficient resources to execute on that program, and 36 percent, in other words, 64 percent do not, 36 percent believe that privacy is important to the brand or market image.

It's in that last category, that's where it's all at. If you believe that it's about improving your clients, your customers, your consumer, your policyholder then you're walking the walk. It's about baking it into your market image and brand.

Now let me do a deeper dive in that question. The question in the benchmarking study is whether privacy is an important part of the company brand or marketplace image. Those that responded yes are different than the companies that responded no or unsure.

For example, the yes group seemed to have a higher likelihood of a formal outreach to new customers and business partners. For some of you in the room, if you're a chief privacy officer here's some good news. If you answered yes, you probably had more resources allocated to privacy as a way to generate money.

MR. PONEMON: If you answered yes you had closer involvement from your senior executive team like the CEO and the board. This is especially true when the program was linked to measurable goals or ROI.

If you answered yes, interestingly enough, you were less focused on control, especially over customer-centric information. I'm not sure if that's a good thing or a bad thing. If you answered yes you had more restrictions on data sharing, especially with third parties, and the notice as well as the policy was written more clearly.

Now, this is the one picture is worth a thousand words. This is probably its own conference and clearly you can't read it but I just want to tell you what this is about. This is something that if you really want to get a big yawn tonight, if you want to sleep well, read this.

It actually takes a lot of data from three very large scale studies that our Institute just completed, one for retail banking, one for the grocery store industry and one for retail pharmaceutical companies. And what we're able to do from about 22,000 observations, remember three different studies using a meta-analysis, we can compare and contrast those companies that are viewed as trusted organizations against companies that are viewed as not being particularly trusted. This is by industry. So, for example, this would include banks, grocery stores and pharmaceuticals. But it was remarkably consistent.

Now, let me just take two of the items of the five items, like notice, security, choice and consent, access, and redress. The companies that were most trusted did a Procter & Gamble. In other words, they baked privacy into the brand. If you have a brand like Pampers that's going to have more meaning if you're shopping for Pampers than if, in fact, you see the Proctor & Gamble name. So brand focus privacy was considered a good fact.

A bad fact under notice was just differing online and offline privacy policies.

On choice and consent or permission marketing related issues, the confirmation that the customer’s choice is being honored was considered something that increased trust. No data sharing, by the way, I know you’re going to throw things at me but that was actually the number one factor on trust but I know it’s not necessarily realistic. No data sharing with third parties was considered a trust-enhancing factor.

Clearly defined opt in on all personal contact including research was especially true in the pharmaceutical industry. It may not be true in banking and the grocery store industry.

But here’s an interesting finding. Choice that is delivered as a categorical variable, in other words, not a simple binomial yes and no was considered a good thing. Give the customer more choices in terms of how that information is being used.

So having categories of use rather than a yes or no is considered a good fact.

Then there’s access and redress. Keep in mind that we found differences between those organizations by a given industry that are viewed as trustworthy or trusted and those that are not.

We also have a broad category called neutral. Things that we think enhance trust like the existence of privacy seal programs don't seem to make a difference. So if you're interested, start looking at this good stuff.

The whole model that we have all talked about, and this is preaching to the choir, is that it's not about just being altruistic and respecting privacy, it's about getting better data and it's using that data in ways that lead to greater efficiency in the organization.

The best model, and I've talked to lots of folks who are on the CRM side of the universe, is about self-service. It's about a customer someday actually choosing what kind of laptop or what kind of printer they want to buy. That exists today.

In order to do that right you have to understand how that customer thinks, believes, behaves and will buy. In order to do that you need good data. In order to get good data you have to be trustworthy with that data. You can't slip, not even once.

So the whole model is moving from availability to ultimately your system and your CRM process generating advice and that leads to greater loyalty, greater convenience and a bottom line result for the organization.

The next step is we have to measure what we are talking about here. We have to convene groups to develop real ROI models that we can demonstrate to the CEOs of our organizations to show that it’s not just about compliance. It’s about generating a healthier bottom line.

If we do it right, we’re going to get better business. Well-defined models are important. Empirical testing of that model to prove the value proposition, and then having workshops like this workshop to educate and to make organizations feel like there’s another way to prove the value proposition for privacy. And with that being said, thank you for allowing me to talk a little bit longer.

MS. OHLHAUSEN: Thank you very much, Larry. At this point I’d like to prompt the audience. I’ll start off with a few questions that I have.

One of my questions is that for some of the benefits that have been discussed it seems to me that they can be obtained with using data in the aggregate.

For example, if you figure out the people who buy diapers often buy, for example, headache medicine you can generate a coupon at checkout or something. As a mother of four children I link those two together very easily, and so I was trying to figure out sort of when you decide when it’s better to sto-3 -4teo0ou ejw questions that I have.

aggregate.

MS. SCHANTZ: The old diapers and beer example. I'll take a stab at that. You can certainly gather information and use information effectively at the aggregate level. That's what we talk about from the segmentation perspective.

Larry talked about working with Peppers and Rogers a lot and they have coined the phrase, one to one. So you hear from a lot of customers that they want to be interactive with from a perspective of what is important to me.

I'll give you a statistic that the Gardener Group has recently produced a report that talks about how solicitations or interactions, I should say, with customers when you do campaign mailing, which is done on the aggregate typically, the success rate of that is typically around three percent.

customer actually contacts the company and you can follow up with a discussion using data that is relevant to that individual who has contacted you. The success of those interactions are a whopping 40 percent.

Studies like that are showing that while you do thought about malaria but because the timing was right the next day I went and got all the shots before I went on the trip.

So if the advertising is done in context when a consumer is likely to be very amenable the percentages, the numbers show the results. There are a lot of other ones that are coming out and I put some on the information that I gave out. It’s showing that the payoff numbers are there when you get down to the individual level.

MR. ABRAMS: There’s a Welt Anschauung issue here that goes back to basically how you think information systems should be regulated. All systems should be secure. There’s no question if you're collecting personal information, you’re matching personal information you should have secure systems. So let’s put that piece of the equation aside.

There's no question that when you have real data and we’ve heard that from the first session this morning, when you have real data that you match together in an accurate fashion and you use that information to build your analytics you end up with much more accurate results.

If you apply that information in a responsible way that builds trust and you are accountable for applying it in a fashion that builds trust you will get better results.

The concept that we can deal with regarding median data or we can deal with data that is aggregated together -- we don't know and therefore we can’t get the history behind some of the events -- leads to less results but it does have a much more controlled environment. The less data that’s matched to individuals, the less fear that that data will be misused.

The question is in an information age are we going to regulate the collection of information? Are we going to regulate the application of information? Are we going to focus on accountability for using information responsibly and protecting information responsibly or are we going to go with a system that thinks in the ways the technology was built 30 years ago, single systems that can do a single thing.

I think that in an information age we really have to think about accountability for the misuse of information and accountability for having secure systems rather than trying to go back to the concepts that made a lot of sense 30 years ago.

MS. GIVENS: I'd like to add onto my Ralph Shopper story to give my perspective on the excellent question of aggregate data versus specific, personally identifiable data.

I think this is a good place where you can build choice into your customer relationship marketing model. I'm able to shop with a discount card and I don't have to identify myself. I think there are a lot of people who would just as soon do that.

But this is a case where if I wanted to and, of course, I had to be a little assertive to do that mind you. One manager didn’t want me to be an anonymous shopper but I think that when you have the opportunity to give a choice you should and still let people have benefits of certain programs. They can choose to be an anonymous user and feed in their data in aggregate or they can choose to receive marketing solicitations as an identified person.

I will add, however, that I think it was a Wall Street Journal article earlier in the year found that people aren't actually saving all that much money, if any, with the supermarket loyalty programs when compared against those companies that do not use them.

MS. OHLHAUSEN: Anyone else want to weigh in?

MR. SAVARD: Yes, I’d like to add something on this, Maureen. Aggregated data, while it certainly has applications with regardehn9Hwethingo0001d feed

Retailers today try to market to customers that are hundreds in size and in segment. To do that effectively you need to be able to have individual level data that's aggregated in some sort of way that makes sense and is accessible.

Some retailers have clienteling programs. We have one at Bloomingdale’s where we have a one-to-one, to further protect consumers’ privacy against these illegitimate and unethical marketers? I mean, part of it I think, goes back to what Beth is saying, it’s the deception is the problem and not necessarily a privacy violation but when they involve privacy violations what steps do you think might be available to us?

MR. ABRAMS: I’ll start. I mean, one of the things that I think we really have to come to grips with and it’s something that Commissioner Thompson and I were chatting about just before the session started is that we have to have a better sense of what we agree is unfair practices.

The Federal Trade Commission has done a great job of defining what deceptive practices are. We understand deceptive practices, but when it comes to things like pornographic sites, pornographic e-mailers, body enhancement e-mailers, not honoring my opt out but rather using my opt out as a sense that there's a real live person at that site, I mean, we have to have the ability to come quickly to a decision on what are unfair practices in a very complicated market and where there is growing consensus on harm and then be willing to deal with the court process around that.

I think that that is one of the things that we need to do because we can pass 16 additional laws that outlaw bad people from doing bad things but if we can’t catch those bad people those bad people continue to pollute the market.

MR. PONEMON: May I respond too? Really there are two issues and they’re separate but related. You have the issue of the bad person doing bad things and the way around that is to create transparency. Some mechanism or mechanisms to show, to prove, that you are doing what you say you will do.

The policy is just a start. Policy doesn’t really have a whole lot of meaning if you’re a pornographer, money launderer, whatever. I mean, if you’re trying to commit evil you’re going to do it with probably a very nice policy maybe even a seal on your website. Who knows. But the end result is it’s about transparency. That’s the key variable.

Now, by the way, I’m not sure exactly what that means. It may be great access to everything or maybe there are different types of seal programs that can be created but at the end of the day it’s transparency for the bad guy.

The good guy still will slip up and make mistakes and big organizations make a lot of mistakes because they’re big. It's about having an ongoing process to measure your success. It's about trying to make those mistakes smaller and less frequent.

So these are two separate issues. And frankly when a big company makes a mistake I think it’s more damaging to the privacy clause than when this smaller fly-by-night companies make mistakes. When you’re dealing with a major brand it’s much more costly than a fly-by-night.

In a way it’s the buyer beware issue. If you’re buying a product and you don't know who you’re buying from even if the site looks cool at the end of the day it’s your choice. If you want to give them your credit card I suppose that’s a choice you make as an individual. But when you’re dealing with a major bank or a major consumer products company I think there are certain expectations that we have.

MS. HUGHES: I’ll put another spin on that, too. I mean, these are ways that you can really get at that issue but I think education is another thing. I mean, education for the public, the end consumers.

The FTC is trying to do some of those things. We’ve got other organizations like BBO where we’re trying some education stuff through the Ponemon Institute and things like that.

Also, I think, the media can play a role here because you have these examples of the bad guys are the ones who do things wrong. It would be really great to see well, here’s things you consumers need to know or things you could do differently to offset these things.

So take the bad that’s always in the press but then add some education with it and I think through that then, through all these different channels that we should be able to do that.

fearful.

Then they oftentimes these days if they have Internet access are going on the Web and they are finding very specific consumer education resources to help answer their questions.

The Federal Trade Commission's website is a very good example. Also, it's a good example because it has some information in Spanish. I will say that the web is unfortunately not good for those who don't have computer access and are not comfortable with computers. But I do think that consumer education in some respects is better these days.

I would like to add, in answer to your question, Maureen, I think most of the people in this room will not agree with what I have to say. But as a consumer advocate, I think more FTC enforcement, making examples of some of the bad players, and also making it easier for consumers, those who have been truly harmed to sue, to go after the bad guys would be good.

I think that the Telephone Consumer Protection Act, which gives us the ability to go to small claims court and sue telemarketers, junk faxers, et cetera, has had some good effect. I think that that is one way to answer your question.

MR. SCHRADER: I'd like to add one other point.

The one argument that I hear that seems to be the most obvious but I don't hear it at all so I want to bring it up is hit them in their pocketbook.

The reason why we have so much spam is that the cost is very low. I saw an ad two weeks ago you could send 28 million e-mails from $149. Now, if you're a marketing person what a wonderful opportunity, right? What person wouldn't want to go for that?

But if we could get to the point where the cost of sending an e-mail commercially was approximately in the same ballpark as the third-party mail or any of the other traditional marketing vehicles I think the problem goes away by itself because that $28 million for ten cents or a nickel would be $2.8 million or $1.4 million for that spammer and the spammers and rogue marketers don't have that kind of money.

So the free market solution of getting a price on the cost but not to mention the consumer side cost of having not to clog up the mailboxes. I think that alone would take care of the problem.

MS. OHLHAUSEN: I wanted to fit in another audience question. I'll throw this out to the panel in general. Where today is there a working model in industry that correctly balances sharing information and privacy?

MR. ABRAMS: You mean which companies?

MS. OHLHAUSEN: You could say a type of industry or if you have a specific company. They didn't specify.

MR. ABRAMS: I would say I work with a lot of companies who have looked at privacy from a strategic perspective rather than a tactical perspective. I think the companies that look at privacy from a strategic perspective, and I think it's backed up by the data that Larry has put on the table, are always looking for where the balancing point is between the appropriate application of information to create value and how their customers are going to see that application of information. They use that to build the processes in place for balancing the use of information and privacy.

I'll go back to the simple equation which is the beginning point that trust is the component and trust is first based on the value you create for the consumer based on your use of information, making sure that it's always secure and applying the information in an appropriate fashion or manner.

Smart organizations have similar metrics that they build into their organization, similar guide points that put them into that constant balancing position. Organizations that are not looking at privacy strategically but rather looking at it tactically, what are the two or three laws I need to abide by and how do I abide by it, are having a more difficult time finding those balancing points.

MS. OHLHAUSEN: Are there some industries then who are sort of generally ahead of the curve in that and some that lag?

MR. SCHRADER: Definitely. When I was pulling together information on case studies, many of which are on our website, it struck me that a lot of the international banks, even those dealing with European regulations, are doing an appreciably better job than, I think, banks in the United States.

Examples would be Union Bank of Norway, National Australia Bank, Royal Bank of Canada. There’s a Harvard business review case study that was published on how they use it.

My main point in answering the question would be the two ways of balancing it would be what are the conversion rates, so that’s a measure of how accurate and precise the marketing people were and then what are the customer satisfaction rates?

If a company can get their conversion rates up and the customer satisfaction rates up, which those three companies have done, then I think it’s a win-win on both sides of the equation.

MS. OHLHAUSEN: Anyone else? Larry?

MR. PONEMON: There are two models that I think are appropriate for measuring the value of privacy. One as I mentioned in my presentation is to do the conventional ROI model and CEOs love it. They'll ask the question what is the ROI and how can I measure the impact? If I spend a dollar on privacy will I get ten dollars back or three dollars back? So that's the conventional way of doing it.

The problem is a lot of the measurable issues are difficult because they're longer term. Another approach, one that is not as common, is like a quality or a total quality management(TGM) approach where you can measure impacts, both positive and negative impacts.

Both models are actually being tested in a number of different organization and a number of different industries. Organizations that have the greatest brand, that have the greatest market image at stake are probably in a position to demonstrate value through ROI and TQM.

Organizations that are not as brand-centric, consumer focused, will have a more difficult time. But it is not an easy exercise. That's why in my last slide I think there needs to be a pool of companies working together to put together that type of framework to justify that value proposition.

MR. ABRAMS: If you go back to the basic research done by Alan Westin decades ago, he isolated the fact that there is a relationship between the amount of information the public will accept you using and the value you create for them with that use of information.

That concept is not new and it’s a concept that we have understood in the privacy profession for 30 years. How you constantly put that into the process and put it in play is the strategic concepts behind good privacy management. People don't go to a brand because they do privacy well. They go to a brand because they are trusted, because they create incredible value. The other pieces enhance that.

It really begins with a focus on using the information to create value for the consumer which creates higher levels of satisfaction and increases profitability.

MS. OHLHAUSEN: Well, I hate to say we need to wrap things up here to keep on the big schedule but please join me in thanking all of our panelists for a very interesting session.

(Whereupon, a short recess was taken.)

MR. ZYWICKI: For our final panel today we’re going to have sort of a multimedia presentation. First, We’re very pleased to have Commissioner Thomas Leary here from the Federal Trade Commission and he’s going to kick off our final session of the day just by saying a few words. Commissioner Leary.

finding out something about.

One of the things that we have the capability of doing, with your help, is collecting information on costs and benefits associated with sharing of consumer information in a commercial context. That doesn’t mean that we are capable of resolving all of the value judgments that may be associated in that field. We’re not necessarily capable of even quantifying them or attempting to quantify them. But our basic pitch, our basic message to you is that people are better off with more information about things like this rather than less.

Let me give you just a very, very simple analogy. I doubt very much that anyone in this room will buy a house on the basis of the lowest cost per square foot of living space. I don't think that people make ultimate decisions on something of that importance simply based on statistics.

However, I think that probably everyone in this room would feel better informed when you were making that kind of a decision if you knew something very basic about to private school in that neighborhood, et cetera.

What is likely to happen to the costs and the selling prices of the surrounding houses? What does the rest of the neighborhood look like? All of these things can be pertinent to your evaluation and they may be able to be reducible to some kind of a number which will help inform your decisions.

So as I see it, that’s what we’re about here today. We want to see what information with your help we can put together in order to aid decision-makers who have to decide these things. There are many other values involved when you’re talking about an issue like this you’ve got privacy considerations. You've got First Amendment considerations. You have considerations of the value that maybe people place on human freedom to do things or not do things.

All of these things are intangibles that may ultimately drive someone’s bottom line determinations. But it’s always a good idea, if you're deciding on something on a policy ground, to be aware of the price that you are paying if you go down that road. That’s what we're about and that’s what we're here to listen to you and I wish you well, and I thank you for being here.

MR. ZYWICKI: Thank you, Commissioner Leary.

(Applause.)

MR. ZYWICKI: My name’s Todd Zywicki. I’m the Director of the Office of Policy Planning here at the Federal Trade Commission.

I wanted to thank Maureen Ohlhausen who is the Assistant Director of the Office of Policy Planning for her hard work in putting this together. I want to thank all the Commissioners but especially Commissioner Swindle and his staff for their enthusiasm and commitment and input into making this program today such a smash success.

I think that as we look back over the course of the day, one thing that emerges is that the question that is often phrased in the popular press or in many people's mind should we trade off privacy for convenience is really not the right question in most situations. In many ways it’s meaningless to pose it at such a high level of abstraction.

I think what we’ve heard this morning is that there are many situations where consumers benefit, often in

f-is ng1 T13

t h

I recently saw a survey where they asked people would they be willing to get to the airport 20 minutes earlier for increased airport security and a majority of people said yes. They asked them would you be willing to get to the airport two hours early for a flight for increased security and very few people said yes.

Immediately following this panel Wayne Abernathy, the Assistant Secretary for Financial Institutions in the Department of the Treasury will be presenting closing remarks. So we'll just go straight from this panel into his comments once he gets here around 4:45.

Our group on the panel will be first Michael Turner who is the President and Senior Scholar of the Information Policy Institute. Michael Staten who is the Director of the Credit Research Center, Georgetown University. Robert Hunt who's an economist at the Federal Reserve Bank of Philadelphia.

Solveig Singleton, Senior Policy Analyst at the Competitive Enterprise Institute. And finally, Professor Peter Swire, Professor of Law at Ohio State University. I will turn the podium over to Michael Turner.

MR. TURNER: I'd like to begin by thanking the FTC for their leadership on this issue and for Te8 0 TD0 Tc(14)Tj/TT2 1

credit scores against different types of data but we controlled for quantity and quality of data. I'm going to get into that when I discuss the scenarios we developed based on state legislation in our full file case study.

But essentially, we looked at the relationship between preemption and the quality of data in the report and I would add to that the quality and quantity of data in credit reports, and then, again, the relationship between the quality and quantity of data reports and access and price to credit.

Now, the three case studies we examined dealt with automated underwriting and here we're discussing consumer mortgages, prescreening, which in the context of credit cards only, not insurance, and then full file credit reporting and the ability to risk model, assess risk.

In terms of the prescreening component we surveyed seven major credit card issuers. Here I will state for purposes of full disclosure this was not a random sample of credit cards or credit card issuers. We worked with a group of companies who have already organized around this issue and surveyed them as well as other credit issuers with whom the Information Policy Institute has a relationship.

However, we feel very strongly that this is a representative sample both in terms of firm size and for

action.

In the first scenario we held constant the type of credit that would be affected. It was revolving credit, credit card credit. But we varied the firms’ size so small and medium and large data furnishers dropped out.

In the second scenario, scenario B, we held constant firm size, only large furnishers dropped out, eight large furnishes, but we varied the type of credit and it was revolving and nonrevolving credit so it was credit card credit, auto loans, boat loans, home loans, student loans.

In terms of the number of files we purged, in the first scenario we had 13 percent of trade lines were purged. In the second scenario it was 21 percent of trade lines were purged. So this was really the impact on the quantity of data being provided in a voluntary system. This is important because if, in fact, a private right of action is introduced in a voluntary system there are some furnishers that may drop out.

There are reasons, different reasons but very good reasons, to believe that maybe small and medium-sized data furnishers who don’t have the wherewithal to withstand a legal challenge on one hand. On the other hand it also may be very large data furnishers. Certainly if I were an enterprising young lawyer and I had an ability to build a class-action lawsuit against a data furnisher, I'm going to target a Citi or a Chase or a large furnisher and not the community bank of the local credit union. So for that reason this is why, this is basically the rationale for varying our scenarios.

In the second two scenarios we looked at state proposals, and again, all of these are based on state proposals that have been introduced this year. We looked at basically accelerating the obsolescence rate for derogatories which is jargon for, in essence, you purge negatives, late payments, delinquencies. Instead of maintaining them for seven years you maintain them for only five or four years.

Similarly, public record information, for example, if you file for bankruptcy, or if there is a tax lien against your property, is maintained now for at least seven years. There are proposals that would either purge this data after three years or, in fact, upon payment/F1 1 Tf-4.2 0

propdatato aormation, for

prn fare prf.ffollow Tcr four years.

models and this is important. We had four commercial scoring models from two credit bureaus, from TransUnion and Fair Isaac and two credit scoring models from major credit card issuers.

We then constructed basically using this we ran 3.6 million actual credit files against these four scenarios so the data was modified according to these state proposals. We were then able to measure the impact on the predictive power of these models, the impact on the number of scores that were affected and the impact on the decisions in the case of the score or the credit card models whether they were accepts or rejects.

We were able to compare this in both cases again because these were actual credit files, 3.6 million actual credit files taken from December 2000 and December 2002.

and information tools I think it’s also important to talk about some dubious methodology. Here I’m referring to an argument that you've all heard, even today, in the context of prescreened offers of credit and identity theft.

Well, this argument runs thus. There have been more prescreened offers of credit in the mail and the incidence of identity theft has also increased. Therefore, they must be linked. That’s co-variation. In Economics 101 they teach you that the hemline of a woman’s skirt rises with the increase in the Dow Jones. That’s co-variation. They're not related.

This has been touted in front of the House of Representatives in testimony by Joel Reidenberg who said that dumpster divers are diving into your trash to get your prescreened firm offers of credit. It’s good that it’s dumpster divers because that’s rubbish.

There’s nothing in a prescreened offer of credit, apart from your name and your address, that would be of any value to a would-be identity thief. It’s the same information that comes to you on a Time Magazine or, more germanely, an issue of The Economist.

There’s also in the issue of Privacy Times that came out two days ago in the article about organized criminals stealing the prescreened firm offers of credit, there’s nothing causally that links these two. In fact, in my study, I show how prescreened firm offers of credit have a much lower incidence of identity theft than other forms of application fraud.

Another dubious methodology is this notion that Vermont, California and Massachusetts are exempted from the strength and preemptive provisions of the FCRA and are outperforming many states despite these exemptions.

Well, here again, this is a little misleading. In fact Vermont’s exemption deals with affiliate sharing and has nothing to do with scoring. It has nothing to do with how your mortgage rate is set.

California and Massachusetts, again, an incredibly narrow exemption from the preemption provisions dealing with data furnisher liability but there's no private right of action. They have no disincentive to impact data furnishers from providing full file information.

This is misleading and it is harmful to policy. They are bound by the strength in preemptive provisions. They are not exempted from the preemptions in the FCRA. The citizens of these states enjoy the benefits from the uniform national standards of the full file credit reporting system in this country.

Some serious methodology you also heard today, the Consumer Federation of America study. This, in fact, was an excellent study. The scientific method was applied. There was a very robust sample, a representative sample, and there was a sound interpretation. Unlike other studies I referenced, there were no quantum leaps of logic in this study.

This is a study that needs to be given serious consideration and I would like to say, inasmuch as I have worked very intimately with the Consumer Federation of America and Consumers Union in the work I do in media ownership, I’ve always admired CFA’s adherence to the scientific method and their use of data.

We filed comments before the FCC on media ownership and collaborated with Mark Cooper from Consumer Federation of America and Gene Kimmelman from Consumers Union.

I can’t get into the findings, unfortunately, because I’ve been told to stop. I will actually respect the rules, but the findings are all in the study. I would be happy to answer any questions about the findings. I’m sure you’ll see them in the trades, both good and bad, hopefully for the better. But I’d be happy to meet with you afterward as well. Thank you very much.

MR. ZYWICKI: Thank you, Michael. Now Mike Staten from the Credit Research Center.

MR. STATEN: Thanks, Todd, and thanks also to the

The more we listen to events like this and panels their ability to collect data. We tried to define what those restrictions would be to help clarify the process, what would it mean for their operations, what would it mean for the consumers that they served. That's essentially is and is continuing to be our methodology as we move through these cases.

So basically we have three objectives. First of all is just simply to determine all the different ways that personal information was being used to deliver products, services and value to consumers. That sort of highlights what is at risk.

The next step was to determine the impact of opt-in rules and I'll tell you about that in a second because we wanted to try to clarify what we meant by opt in as best as we could. What would be the impact on company operations and in so doing all of this we eliminate the cost of additional privacy. We must identify what's at risk if opt-in rules prevent or interrupt those data flows.

Most of this in the case studies that we conducted is qualitative but we tried to inject quantitative estimates wherever we could get data that would help us do that.

I co-authored with Fred Cate. What we intend is for all of these cases ultimately to be collectively joined. We selected our corporate subjects to try and get at different dimensions of data usage, much as the way the panels earlier today were assembled. You got different slices from different kinds of industries. The ways that they used data and what they're providing their customers and the implications of opt in are a little different as you move across different industries, different companies within those industries.

Let me just spend a second talking about our subjects. This has been a project that has been underway for I would say two and a half years probably. We had the great advantage of starting this project right on the heels of corporate attempts to comply with Gramm-Leach-Bliley(GLB Act).

In fact, if we tried to do this, I suspect, five or six years ago we would have not made nearly the progress that we were able to do this time. One of the things we found out as we started our interviews was that most companies a couple of years prior to our talking to them wouldn't have had any idea of what they were doing with personal information in terms of all the different units of the businesses.

That was one of the great almost herculean efforts for some companies was to convene all of the different units of the business and have extended discussions themselves as they tried to comply with GLB Act to determine how information was being used and the privacy implications within their company operations.

Fresh on the heels of that, it made these interviews go much easier because they were already accustomed to thinking in these terms. Nevertheless, we found that they were learning during the process of our interviews just as we were. Sometimes all we did was just sit back and listen to them talk amongst themselves.

The very first company that we tackled was in financial services because so much of, as you've heard earlier today, so much of that business is information driven.

In some sense since we abandoned the days, as Pete was referring to of a hundred years ago, where Wells Fargo was toting gold bars back and forth and cash, all of its information now is in the sense of digits being transferred from one account to another. So it's all about information flows in terms of the products that they're providing.

The financial services industry is almost the epitome of an information-driven industry. You would think privacy would be at the fore and certainly it is, and we've heard that companies are aware that it is.

So we wanted to understand just the role of personal information in extending credit and other retail financial services. We picked MBNA. We picked them for a very specific reason: because they’re the epitome of a startup, a company that didn’t exist 25 years ago and has gone from essentially well, I’ll say, 600,000 accounts when the company was created as a spinoff unit of Maryland National Bank back in 1980 to over 50 million accounts in less than 20 years.

Now, they did all of this without any physical brick and mortar presence. No branches. They reached out and they touched customers across the country and now overseas and they did it by managing information.

It’s an incredible example of how targeted marketing frees a provider of services, in this case a lender, from brick and mortar constraints and allows them to compete for customers, 2000, 4000, 6000 miles away without ever having met the customer and yet can do that with enough confidence that the customer will be interested in their offer and, in fact, will pay them back when they make them unsecured offers of credit. That’s a pretty bold risk, and they were able to do it very successfully0 Tc(8)Tj/TT2 1 for example, and are able to target consumers effectively.

It has boosted competition in the credit card industry, and we heard something about that earlier today. So it’s a very good example of the boost to opportunities for consumers through the competitive market associated with firms being able to use information to target market.

So that’s really the focus of the MBNA case. That was the first one we did. It’s completed. The article that we wrote on that is actually forthcoming any day now, literally, in the Duke Law Journal.

The next case we tackled was Travelocity. Here we wanted something in the online environment so we picked an online service provider. This happens to be, as you know, a database-driven travel marketing and transaction company. It customizes much as we heard earlier today from Bluefly, for example, it customizes travel offerings based on personal information and clickstream data from customers browsing sessions so that it can tailor banner ads and different promotional opportunities to customers that have visited the website.

In so doing, this is really the company’s words now, it delivers personalized travel service to 30 million members faster and at far lower cost than would be possible in the physical shopping environment. It’s essentially brought a individual’s own personal travel agent to that

affiliates or sometimes not even affiliated in terms of ownership but nevertheless are operated under the brand name.

What happens if you interrupt those data flows as would happen under various proposals for opt in or opt out associated with affiliate share. That's the focus of that case.

The fourth case we decided on, actually after we had started all of these and started realizing how a lot of these firms were using information and where they were getting some of this information, and we realized this whole issue of third-party data is sort of a black hole to us. Or at least it was a black hole to me, and I didn't fully understand where this was coming from and so the fourth subject of our case studies was Acxiom.

As one of those information aggregators out there that you've already heard about to a great degree earlier today Acxiom pulls together and aggregates information and then provides it to clients. By their own statement they have third-party information on 95 percent of U.S. households, 13 million U.S. businesses, 70 million properties throughout the U.S. This information is used we discovered in lots of very interesting ways that we had no idea about.

It's used to accurately identify customers and

data that other firms are acquiring to do many of the things that you heard about earlier today.

Part of the methodology is to try and to conceptually impose an artificial constraint on the information flows as they exist today. So we wanted to try to analyze three different opt in scenarios, ranked here on this slide from least restrictive to most restrictive.

Least restrictive in our taxonomy would be opt in for third-party sharing which we have - it’s probably the most commonly proposed out there. It’s not something that has occurred yet under GLBA but has often been proposed as a supplement to GLBA. We’ve got opt out under GLBA right now for personal financial information. But this would be opt in that would require explicit customer consent for any sort of third-party sharing.

MR. STATEN: The second most restrictive would be opt in for affiliate sharing which brings it a little closer to home. This is affecting now information that companies already legally possess among their affiliates and then finally blanket opt in or permission-based marketing as it’s sometimes called. The restriction on information used for purposes other than that for which it was collected.

Basically, one of the components of this set of case studies is to assemble as much empirical information on the impact of opt in itself. Why opt in poses such an obstacle for information transfer, largely because of the nature of the default rule here that it’s very difficult to get customers to consent or to even recognize or respond to invitations to consent for these kinds of offers.

Over 50 percent of unsolicited mail is not even opened according to the U.S. Postal Service. So many times if you put out an invitation to opt in to something, you’re not even going to get your message heard by the consumer.

So we try to incorporate that into the methodology here where basically we model opt in as essentially setting the information flow to zero. Then we go back through the different uses to which the company has put the data and determine what then goes away in terms of benefits or elements of their operations if that information is shut off in each of those different scenarios.

I’m getting the hook here so I’ll resist going on with the rest of my slides which really left methodology and went into results anyway. I couldn’t resist putting them in but we’ll save that for another day. Thanks.

MR. ZYWICKI: Thanks. Our next speaker is Robert Hunt from the Federal Reserve Bank of Philadelphia.

MR. HUNT: So I think I’m the only person here today that has to issue a disclaimer like this. These views are my own and not necessarily those of the Federal Reserve Bank of Philadelphia or the Federal Reserve system.

About a year ago I had the opportunity to interview the manager of one of the credit bureaus in Sweden and he was explaining to me that under Swedish law you can only retain derogatory information for something like three years. I asked him well, is that a bad thing? And he said, no, not really because Swedes don’t borrow anyway.

Back to the U.S. There are two problems that confront lenders. The first we call adverse selection, that is how well do I distinguish between borrowers of different risk. That’s going to determine who gets credit, how much and on what terms. The other problem we call moral hazard. How can I induce the borrower to repay once I have decided to give him a loan?

Well, if I don't have collateral to take, one of the few tools I have available is reputation. If you don’t pay the loan I’m going to tell all the other lenders out there that you're not very good about paying your debts.

It turns out credit bureaus are able to mitigate both of these problems because they provide information that improves the assessment of risk and the pricing of credit risk, and, of course, they are the mechanism for implementing reputation as a way of convincing borrowers that their payment histories matter in the future.

What is interesting about credit reporting in the United States and we’ve said this a few times today is that what we have is a voluntary information sharing equilibrium. This is actually kind of a puzzler because it’s not, a priori, sensible for lenders to be sharing this information in the first place.

There are trade offs. On the one hand if I have more information about the customers of my rival that means I can do a better job of making an offer to them and as a result I will get these customers and I will earn profits on that. But there’s a cost and that’s because the rivals are doing exactly the same thing to me and that means I’ve got to compete more aggressively to retain my own customers. That means I earn less profit. So at the extreme a voluntary equilibrium may not happen. If there's too much competition lenders are not going to share information.

One point that comes out in the working paper that is the basis for this talk is that the U.S. experience is due in part to the structure of retail and credit markets that we had 50 or 100 years ago. This is rather different than you see in other countries and it might explain why in many other countries they had to legislate credit bureaus into existence rather than to have them arise voluntarily.

Another interesting feature about this is that credit bureaus exhibit network effects. Joining a bureau is more attractive if it already has many members because if I get a credit report it means I get a comprehensive snapshot of the borrowing habits of a person.

What this means is that it’s hard to set up a bureau but if you have any success there tends to be a bandwagon effect. Everybody joins along. That also means there’s a tendency towards a concentrated credit reporting industry.

When should we expect to see credit bureaus, that is, when should we expect to see this voluntary equilibrium? When you have conditions that are conducive to a lot of unsecured lending that helps you amortize the fixed costs of establishing these bureaus, when lenders are small relative to their market, that is, when lending markets are not very concentrated or, for example, when people are mobile. In that case lenders don't know everything about the entire universe of potential borrowers that they encounter.

When the landing markets are fragmented either geographically or functionally as they were in the United have added to this slide is that historically credit bureaus were also fragmented geographically and functionally over time and this changed over the century.

Finally, when people borrow from many lenders at the same time because this creates an externality. Each loan I take out changes the probability that I'm going to be able to pay any of my loans. Lenders want to know that.

Now, one of the issues that we've talked a little bit about today is the accuracy of credit bureau information. Now, we know it's valuable because lenders are willing to pay for it and they use it in automated credit decisions but we don't have a great deal of information about the quality of the information that is in credit bureau files. Until very recently we really didn't have scientific studies. That's just begun to change in the last year or so and you actually heard a description of one of those studies earlier today.

I would emphasize that it's important to distinguish between any error in a credit report and major errors that will affect decisions about credit, insurance, and employment. Not all errors are equal in terms of an effect on a credit score.

The next thing to emphasize is that even a very small incidence of major errors translates into tens of thousands of erroneous credit decisions and that's simply a fact of the number of credit decisions that we make in this economy every year.

Of course, there are remedies for noisy information. You can design a robust credit score. You

So that means they have an incentive to provide high quality data. Credit bureaus, in fact, set reporting standards and they have very elaborate programs for auditing incoming data. It’s also the case that credit bureaus process most of the consumer disputes.

The next question though is does this get us to an optimal level of accuracy? That is, do credit bureaus spend resources on accuracy to the point that the marginal benefit of additional accuracy is equal to the marginal cost?

I would argue very tentatively the answer may be no. This is based on a sketch of a model, not even a model. So this is tentative. First of all, lenders probably care more about what I call Type 1 errors, that’s making a loan on the basis of erroneous information. For example, there was a derogatory that should have been in the file but wasn’t there.

Borrowers probably care more about Type 2 errors. They can’t obtain a loan because there was derogatory information in the file that shouldn’t have been there. Now, it’s possible that bureaus may be more responsive to the needs of lenders than to the needs of borrowers; after all, lenders are the principal sources of revenues for the industry. It’s possible that bureaus are going to be more preoccupied with Type 1 errors and relative to some measure of the social optimum, that means we’re going to get the wrong mix of mistakes.

If it’s also the case that bureaus ignore consumer losses we’re also going to get too many mistakes. It may be the case of bureaus underfunding consumer dispute process as well and the reason is pretty obvious. The bureaus are incurring most of the cost of this process and yet they’re sharing the benefits with consumers.

Now, I would argue that bureaus do subsidize this process. The question is whether they subsidize it enough. Well, is this a rationale for government intervention? In fact, this intuition that I’ve described is contained in the legislative history of the Fair Credit Reporting Act. I would also argue that the Fair Credit Reporting Act is a pretty good example of sort of a sophisticated design of a regulation with costs and benefits in mind. Congress thought about this when they were developing the act in the first place.

The first thing that the FCRA does is establish a custom negligence rule for credit bureaus and users of credit reports. It specifies different standards of care for different parties. For example, for information providers the hurdle is not very high. All you have to do is avoid disseminating information that you know is wrong, and you have to respond to requests to verify your information.

Bureaus, on the other hand, have to take reasonable precautions to ensure that the data in their files is accurate, and they have to avoid unauthorized disclosure. The point here is the reasonable precautions. The fact that there's an error in a credit report is not a violation of the act. Users can access credit reports but only for purposes that are authorized under the act and they're responsible for notifying consumers of their rights under the Fair Credit Reporting Act.

The other thing that the FCRA does is that it specifies different remedies for different parties. For example, a variety of regulatory agencies can sue any of the participants in this process, information users, credit bureaus, or information providers.

However, in terms of people that consumers can sue under the act, that's a little more limited. They can sue information users and credit bureaus generally, but you'll notice that information providers are not on that list.

Bureaus can also sue under the act, but in general they can only sue their customers. There's also criminal penalties for information users and credit bureau employees that violate the privacy rights of consumers. The other thing that the act does is encourage error

already been done and there’s a lot more work to do. This is not a very easy problem because it’s not easy to choose the right counterfactuals for this kind of analysis. And not everything we’re interested in is priced in a market.

I would also emphasize that it’s important to understand the nature of the equilibrium. Institutions matter, regulations matter, financial market characteristics matter.

I’ll give you one example. This is the market share of the top ten banks with credit card receivables over time and you’ll notice that the share of these top ten banks rose about 25 percentage points in the last five years of the 1990s. It’s now at about 65 percent.

Why do I point this out? This is an era when the competition in the credit card market was intense. It's also a period when the largest lenders were sharing information with their rivals and customers were being poached.

It happens to coincide with a period, and we’ve already talked about this today, when some issuers reported less information. In particular they stopped reporting credit lines and high balances. I need that information to run a credit score.

That means there are competitive implications of this. At one point this was affecting one-third of revolving credit accounts. These were some large lenders and it tended to occur more for sub-prime accounts.

So what happened? Well, the credit bureaus and the regulators responded. Basically, the regulators rattled their sabers and the story is that bureaus threatened to enforce the reciprocity rule. If you don’t share credit lines and high balances you won’t be able to get credit lines and high balances back. That’s the story.

I would like to ask the question about how the bureaus actually enforce this reciprocity rule because the $64,000 question is will it happen again? Thank you very much.

MR. ZYWICKI: Thanks, Bob. Next us is Solveig Singleton, Senior Policy Analyst with the Competitive Enterprise Institute.

MS. SINGLETON: Thank you. I’m going to talk --

11

10

10

much. 10

Then secondly, I’m going to talk a little bit about the information flows versus privacy debate and some of the methodology of market failure arguments. Third, I’d like to talk briefly about the slippery question of values versus costs and benefits which the commissioner touched on earlier.

To start the first chunk that I hope to cover, you heard some concrete examples today of how information functions to help companies cut costs, improve security, develop services, offer products, and so on. Michael Staten talked about this, too.

Essentially, these are small pieces of the picture, and I'd like to try to give some rough indication of what the rest of the picture looks like. Basically, what’s going on is this information moving through the economy is enhancing competition; that is, it’s giving consumers more choices.

you see but the things that you don’t see.

With that, I’ll leave this first section of my talk.

Now, I want to discuss the tension in the debate about the flow of information and privacy and confidentiality. Now, in some sense, both the flow of information and privacy are good things that people want. I think it would be possible to say we have some good benefits in the flow of information but as a general rule people want more privacy and we don’t see enough of that. At that point they begin to think, well, maybe there’s some kind of market failure here.

I think that this argument runs into some very, very thorny methodological problems right from the start. First of all, confidentiality is certainly a good as are the other things, but none of these are absolute goods. So how do you judge what their relative value is? How do we judge what the value of privacy is relative to the value of having cheaper credit?

One might say that consumer opinion polls give you some evidence that privacy is, in fact, a greater good than the benefits of information flows. However, those answering the queries of pollsters, to grossly truncate a very sophisticated economic argument, don’t bear the costs of expressing the preference for privacy that they do in the polls the same way they would if they were acting to buy privacy as a good in the market.

For that reason, the vast majority of people who do economic methodology find consumer opinion polls to be a very unreliable guide to what peoples values, in fact, are. That is to say, their actions speak louder than words.

As a general rule, people seem to be willing to take steps to avoid very concrete privacy problems like identity theft. The9,did verint wee sood in Thasecujori,ke tif thedon’tle seem thav benhedeep philosophiceranesoog to

12TTT2 1 T18.2 -2.15 TD-0.0001 Tc0, ontheight also tal abotiy riacy as sorttoTF1

As a general proceeds.

tif tmselvesft.So let’lesiewiy privacy ass.

tifod sayo e, trs.

That ,cIif inkif Thatfnd consumsey wereiablg to

tif theibehavi(Fobss.)Tj/F1 1 Tf-8.2 0 TD0 Tc2(4)Tj/TT2 1 Tf8.2 -2.15 TD-0.0001 T of externalities that would often be produced would, in fact, be negative. That is to say, the benefits we get from using information, whether that’s security, being able to locate witnesses and fleeing judgment debtors, donors to political groups and charities, starting magazines that are targeted at some strange niche audience, those benefits, since they don't depend on the contribution of any one individual's information but instead depend on the functioning of the system as a whole, are themselves positive externalities and have some of the qualities of a public good.

So I think the externalities argument ultimately there doesn’t work, and I think it’s pretty questionable whether you should start to think of property rights in information any broader than those we already have in copyright and defamation and so on.

Finally, there is the whole question of information costs and transaction costs which is a staple of law and economics. I think, somewhat ironically, economists who do methodology seriously have a lot more difficulty with these concepts than lawyers do. That is from Coase and Gordon Tulloch.

Authorities on economic methodology have said that it really is very questionable as to whether you should take a world of zero information costs or zero

precisely because they believe that ultimately the consumer will value the exchange. There are passwords, there are pin numbers. There are good spam filters. There are mailing houses and so on. Most legitimate e-mail marketing, for example, Eddie Bauer, is opt in.

There's not much left for the alleged market failure to fail to provide other than the kind of broad restrictions on information flows that are imposed by law in the European Union, but it’s completely unclear what practical use these broad restrictions serve or why consumers would, in fact, demand them. That is, they are not an effective tool to address any real concrete problems whether it’s spam or identity theft, both of which are largely enforcement problems.

MR. ZYWICKI: Thank you, Solveig. Our final speaker is Professor Peter Swire from Ohio State University.

MR. SWIRE: Greetings. My thanks to Professor Todd Zywicki and the Commission and Commissioner Swindle for sticking with us through the afternoon.

I’m going to start by saying that I love many, many, many data flows, but I don’t love all data flows. Some are not good. Handing out people’s passwords is not good. Handing out people’s Social Security numbers in a world where Social Security numbers are a key to people’s identity is not good. In a lot of settings, data flows may be good but you have to have good protections built in. If you don’t it turns out that having institutions that work well at holding on to that data leads to various kinds of problems.

In this panel in some ways I’m the one who’s going to emphasize some problems with data flows. I’m leaning on that side of my own views to sort of bring out points on methodology that maybe haven’t come out so much thus far today.

I going to make just a couple of points in response to some of what we heard. First of all, I commend Robert Hunt’s paper, which I hadn’t heard until today. I thought it was very elegant at showing why we have the Fair Credit Reporting Act and private rights of action with enforcement, with a whole series of reinforcing rules.

One of the things that we have there is a set of rules that lead to reasonable precautions in the handling of this important data. We have transparency to consumers about how that data is used. It’s because of those factors that we are likely to think that FCRA is roughly efficient.

If it turns out we have other settings where we don't have reasonable precautions in place or we don't have very good transparency, we might have less confidence that we would come anywhere near an equilibrium that economists would say is the right one.

I also have read some of Michael Turner’s paper. I didn’t get to read the whole thing in advance, but there’s much to commend in the careful numbers that have been run there. However, in comparing where we are today to 30 years ago, which part of what the paper does is compare the enormous growth in credit since 30 years ago or ten years ago, 30 years ago there were just a few mainframes. There were no PCs, there were no faxes, there was no e-mail, there was no web. So you would expect information costs to have fallen enormously in an information-intensive industry in the last 30 years. We would expect much greater efficiency in many dimensions.

So I think, and maybe if I went through all the tables it would turn out that the different scenarios do this, but we can’t easily conclude that exactly the rules that have gotten us through the past 30 years are the right rules going forward. A lot about the improvements we've had come from the better technologies, and we may need to be tweaking laws as we go to the next phase because as Mr. Hunt showed the equilibria are going to shift.

What I’m going to try to do in this time is give an overview in part based on an article on efficient confidentiality that’s at these websites. I’m going to take on the idea that the market works and then in some contrast to Solveig Singleton say that there are some market failures that should be included in the cost-benefit analysis.

I’ll try to show what is typically left out of cost-benefit analysis, and I was reminded today that my first academic conference ever was on cost-benefit analysis. That was in 1979. I gave my first academic paper on the subject. I hope I’ve learned some things since but it’s sure been a long time.

Show us the data. This morning I believe it was Commissioner Swindle who asked us to show him the data. One place where we’ve seen data on cost-benefits is a hundred page cost-benefit analysis of the Health Insurance

10

8

analysis, one point in these cost-benefit analyses is where you start is going to tell you what the costs are of getting to a different solution.

So if you assume, for instance, that the individual has a strong property right in the data, then there’s all sorts of costs that it’s going to take to move the customer away from that. If you assume instead that business owns all the data, then there’s going to be large costs anytime you change businesses’ expectations, what Michael Staten called the status quo.

These rules, the default rules, matter enormously here because I think people who have looked at it have come to believe that opt out and opt in differ. We get really low changes from the default rules either way.

That’s a sign of high transaction costs. That’s a sign that bargaining is hard to do and so the default rule we set is going matter. We’re going to be forced, as people, and if I were just going to predict up front the people who thought that privacy is less important, graduate training in economics was the leading indicator for this.

There could be a lot of reasons for that, but one reason is that economists are taught in the first year of economics that perfect competition is a good thing. We’re in favor of that. And by the way, perfect information is the world of perfect competition. The closer we are to matching all the buyers and sellers the closer we are to perfect competition. You get to Pareto Heaven.

job on the panel. Here’s one.

Let’s imagine a telemarketing world and let’s imagine what turns out to be a pretty good response rate today which is a 3 percent response rate to phone calls. Let’s imagine that 17 people out of a hundred just don’t care if they get the phone call. Let’s imagine, which is consistent with polling, that 80 people don’t want to get that phone call.

So the economists would say, well, there’s some negative utility, that’s economist speak for somebody got mad, or their dinner was ruined or something, there’s negative utility from the marketing call to the 80 people.

So our overall question is, do the losses for those 80 outweigh the gains to the three plus to the marketing company? If so, if the telemarketer can make money on three sales they’re going to keep marketing even though there's this external cost on the 80 people who didn’t want to get the call.

If you think it’s possible in telemarketing, it’s also possible with spam where the response rate is .000 -- keep adding zeros -- 37. Lots of people don’t want to get the spam, and they dread going to their e-mail box. We are likely to think there’s negative externalities from being cluttered with spam. That’s even though the spam artists are making money. So the fact that they market doesn’t prove as a society that it’s efficient.

Without trying to defend in great detail, I’m going to briefly just touch on other market failures that you can see in the privacy area. One is that it is very expensive and hard for consumers to understand how data is being used. We know that because we know it’s hard for companies to know how data is being used inside the company. It’s that much harder for consumers.

It’s high monitoring costs for consumers who enter into a contract so if your name or information gets out in various ways you don’t know who leaked the data. This which means that people can gain from using or selling the data, but you as an individual don’t know who leaked it. You have weak enforcement, weak monitoring and likely overuse of data.

There are high bargaining costs for consumers. In a lot of markets it’s really hard for you to figure out a different market on what data is going to be used with the company you’re doing business with.

There’s the externalized cost, and this was touched on a little bit by Robert Hunt, about mistakes in credit reports. The cost of the mistakes are borne by you the individual consumer, but we don't know who leaked the improper data. We don’t know where the problem happened so there's an externalization.

Then another thing that makes bargaining in this space very hard and makes markets less effective is that a lot of the data and the data sharing is done by third parties. It’s one thing if you're dealing with your bank or you’re dealing with your store and they then give out that data and you figure it out. The problem in this world is that it goes from the bank to six other places and from the store to 12 other places and those downstream recipients don’t even know you as a customer.

So if they make the mistake there's not the usual market discipline of angering you the individual. They don’t even have you as a customer. Credit reporting agencies are a famous example where the customers are the banks and not the individual consumers.

So, in short, the size and magnitude of these are hard to judge. We can argue about it but this is at least the homework to go through to see what the possible market failures are in these markets for information.

Here are some other critiques of standard cost-benefit analysis I’ll just hit on briefly. The first one is one that Mozelle Thompson alluded to today which is there might be a real dichotomy between short run and long run here.

When Todd Zywicki asked well, what’s the marginal cost my answer back was that might not capture it all. The marginal trade might be I get a 10 percent discount if I give you more data. But the long run concern might be about privacy, a society where the government knows everything or a society where all data about people is known. That's a qualitatively different society and we might have different views.

A second critique in cost-benefit analysis is something that's been called a dwarfing of soft areas. It's easy to quantify some things. It's harder to quantify others. Privacy is hard to quantify. How much does it bug you if these things happen. That soft stuff tends to get squeezed out in the equation.

A third one, and law professors are familiar with this point but I think real people aren't, is that in cost-benefit analysis violation of rights don't count. So if you thought you had a human right to certain information or a property right and you thought there was some bad thing that happened because your rights were violated, ordinarily in economic analysis the fact that a right was violated doesn't count. It's just how much utility is over here, and how much utility is over there.

So the many different rights-based arguments in year now requires privacy impact assessments for new federal agency computer systems. OMB is supposed to issue guidance. What equivalent, if any, will happen in the private sector? Larry Ponemon spoke earlier about the privacy management process. How is that going to happen? It will happen for the intense brand companies that have their brand on the line but for the other 98 percent of companies in many instances it won't happen as intensively.

A related question is how can the FTC help us along a path towards encouraging the good flows of data and having thoughtful critique of the bad flows so we can have these reasonable precautions and this transparency the FCRA has.

Flows of information between companies that are using the data are not free. I've tried to point out externalities and other market failures. We've heard about I.D. theft. Some flows of data are security breaches. Some flows of data might violate the rights of individuals. It might lead to a society we don't want to live in.

I think the cost-benefit analysis can't be between free flow and the market works perfectly or we have to have opt in for everything, close everything down. I try in my own work, as I know many others also do, to have more nuance and less ideology here, but I hope to have at least touched on some of the questions raised by today's workshop. Thank you.

MR. ZYWICKI: Thanks, Peter. Before we get to my inevitable question about the Coase Theorem we've got a request for our team of Michaels down to the right to give us a brief summary of the findings that they found in their various studies. So, Michael Turner, do you want to tell us a little bit about what your study found?

MR. TURNER: Sure. I'll talk on the key findings from the three case studies. The first case study, in terms of automated underwriting, here are some of the highlights again. Prior to automated underwriting systems(AUS) and automated underwriting systems are risk models that rely on full file credit reports and access to robust data sets, approving alone took approximately three weeks. In 2002 over 75 percent of all loan applications received approval in two to three minutes.

Origination costs were decreased by 50 percent or $1500 per loan. With 12.5 million sales of new and existing homes in 2002 this produced direct savings to consumers of $18.75 billion.

In terms of the efficiencies, the better performance and higher acceptance rates, automated underwriting consistently outperformed manual underwriting or manual underwriting with a guideline both in terms of approval rates, overall approval rates were 36 percent higher using automated underwriting than manual, and particularly for traditionally underserved communities. The one version of AUS used by Freddie Mac accepted minorities at the rate 29 percent higher than manual underwriting even with the guideline.

Prescreening, the second silo, the second case study. Our survey showed that the average cost to acquire a new account using prescreening was roughly $58. When we ran it across our four scenarios, scenarios A through D, the cost increased from $61 to $73.

Now, that doesn't sound substantial but think about when you aggregate it, and again, I'd like to talk about the secondary effects. The marketing cost would

Even if it's only a thousand or ten thousand in this case are going to invariably be lower income Americans, members of ethnic minority groups and the lowest income quintile.

The competitive effect we've seen from prescreening, and this goes to Peter's point about the units of information cost perhaps not being considered, here we looked at between 1990 and 2000. Prescreening just came onto the scene and Michael Staten did some of this analysis in his work on MBNA. This was a company that didn't exist.

Empowered by prescreening you see cycles of competition of sustained competition in the credit card industry. We estimate that this yields, if you hold prices constant from 1997, savings to consumers of $30 billion a year on the price of credit.

Now, this is based on an analysis done by Evans and Schmalensee of MIT and MIRA. I've spoken with David Evans and he's coming out with his price index next year in the update for "Paying with Plastic" and he says in fact that prices haven't remained constant since 1997. They've gone down. So this is a conservative estimate, $30 billion per year.

Our own analysis shows that prior to 1990 or during 1990, 73 percent of all outstandings on credit cards were at 18 percent or more. Only 6 percent were below 16.5 percent. That’s in 1990. In 2002 compared to 73 percent only 26 percent of outstandings were above 18 percent.

On the other end, remarkably, 15 percent of all outstandings were below 5.5 percent. Thirty-one percent were between 5.5 and 10.9 and 25 percent were below 16.5. So instead of three-quarters paying more than 18 percent now three-quarters are paying considerably less than even 16.5 percent. These are real savings. The cost of credit

constant and your delinquency rates are going to progressively increase, or you can hold the delinquency rate constant and with the less information your acceptance rates are going to decrease.

Basically, we measure and plot that for all four of our scenarios and what we see is this, if you hold acceptance rates constant and if you run it across these four scenarios, delinquencies will increase between 10 and

don’t derive any revenue from the sale of their personal information about their customers.

So if you think about the privacy issue the real impact of opt in is on companies who are trying to move information about their customers that they already have in one of their various business units or across their licensed business affiliates back and forth to better serve those customers.

If we accept Peter’s proposition on opt in, which I happen to agree with, the transacting is costly. If you initially assign the rights to use the information to the consumer and the company is tasked with trying to bargain those rights back then effectively that eliminates those information flows under an opt-in scenario.

So what you need to be thinking about is the impact it has on a company’s ability to use information primarily that they already have but may be located at different units.

Secondly is the point that’s been raised many times today and again with Michael’s results. Personal information is used to target market. That brings more competition to market. It lowers barriers to entry and lowers prices, increases options for consumers, increases consumer choice. There’s no way around it. That’s one of the clear trade-offs. If you truncate the ability to use personal information to target market you’re going to give something back in terms of those gains to the competitive markets.

Third point, with respect to information flows and service delivery. Exchange of personal information across the business units is absolutely critical to customer relationship management strategies. Opt in will kill CRM, and there’s no other way around it. If opt in truly erects that barrier, and the stricter the opt in the more so this is going to be true, it will truncate attempts for companies to know and learn more about their customers and establish those relationships.

Fourth point, there are positive externalities for those positive social purposes like fraud prevention or crime prevention will not be sufficient to preserve the maintenance of the database that is paid for through the ability to sell those products for other commercial target marketing type purposes. So those are those positive externalities that may go away if opt in prevents the information flows of gathering that data.

Last point, I guess, is that there clearly is sign of progress in the market. Not only is there technological progress in moving data but there's progress in terms of company sensitivity to consumer preferences with respect to how their data is handled.

So there are many choices that consumers are being given even under the status quo without new, say, opt in restriction. The required opt out choices under FCRA and GLBA, do-not-call lists mandated by state and local governments, federal government, company-sponsored do-not-promote lists.

Actually, many companies now offer choices to customers as to how they want to be contacted, whether it's through e-mail, whether it's through direct mail, whether it's through telemarketing, or not at all. Many companies are being progressive about that because they recognize that it makes a difference. It makes a difference in their ability to attract the customer and to keep that customer over time.

So there's greater sensitivity there and as we heard this morning, that greater sensitivity is going to impose an important new and more powerful discipline on companies to the extent that privacy is a concern of consumers that actually translates into action on their part.

MR. ZYWICKI: Thanks, Mike. That's a good segue into a question I have for the panel which is a question relating to opt in versus opt out. Economic theory, as Peter Swire mentioned, tells us that in a world without transaction costs it doesn't really matter where we start, whether it's opt in or opt out.

That just really focuses us on the question of what the transaction costs are, and I just would address the entire panel, how valuable is this information to businesses versus consumers? How high are the transaction costs, and does either side have a comparative advantage in processing this?

So for instance, maybe if I just think about my telephone company they may have to try to call me four times in order to get me to do something versus a company that has 24-hour customer service and expertise in processing these requests, things like that. What evidence do we have and what's the state of the knowledge on the cost, the transaction cost associated with opt out versus opt in? Michael Turner.

MR. TURNER: In an earlier study that I did I referenced an experience that U.S. West, now Qwest, had regarding encouraging its customers to opt in to share information among its affiliates.

The problems they had were basically thus, contacting individuals in the households that were of age to give consent, actually getting someone to the telephone or to respond to a mail notification and then explaining to them the need for the information that they were sharing and the functions it served.

Their experience was telling. This is a company with enormous household brand name recognition. I mean, everyone knows they're a phone company. Generally, people tend to trust their phone company. They may not always be satisfied with the service but they incurred costs and they tried a number of different methods. They preselected for outbound phone calls. They preselected for inbound phone calls and they did direct mail with and without incentives, where they would give away one dollar phone card and $5 phone cards.

The cost of obtaining an opt in ranged from, and I don't remember the exact numbers, but it was between about $20 and $35 per opt in. It took, on average, for the phone calls, even with those individuals who were most likely to respond favorably and a script written by a Madison Avenue public relations agency, it took about half an hour to explain, on average.

This is incredibly telling. I can't imagine being a startup, a small or new company where no one knows my business, never heard of my company. What would it take to encourage a customer to opt in and give consent to information share in that case?

So for me this is a barrier. If you require opt in, it's going to benefit companies who have high name recognition to the detriment of competition because it will handicap new entrants and small companies.

MR. ZYWICKI: Peter?

MR. SWIRE: I think there's a lot of consensus that transaction costs are high; where you set the default rule leads to very different outcomes. So that means for areas that you're concerned about where you think the data is sensitive, you have to really work through what that default rule is.

In the medical privacy rule, for treatment purposes and payment and health ea5rentM, for treatment whether you go into the hospital directory is opt out.

There was an attempt in the rule to make a guess about where most people would be. Because the transactions costs are so high that's probably the right way to go when there's data that's important to regulate at all. I knew that "regulate at all" would have to get a rise.

MS. SINGLETON: Actually, I have just a very general comment on that. I think one of the things that Coase himself emphasized repeatedly in his very important article in which he creates a model of a world with zero information costs was that the model has extremely limited relevance to the real world.

He emphasized again and again that in the real world the costs that you bear in working out a transaction or getting information are just as much a part of the economic process as the costs used, the amount of resources you expend on the resources or what have you. So when we're thinking about default rules and what the ideal rules are I think that it's important to keep in mind that when you're doing good economic methodology, you don't necessarily get to a better world by forcing, say, lawnmower manufacturers to include with all their lawnmowers a 300-page treatise on metallurgy.

I mean, forcing things to move to a world with perfect information just probably isn't going to be the

elsewhere basically is phrased in terms of two constituencies which is business and consumers and their shared interests or rival interests. But there’s a third constituency which is near and dear to all of our hearts on this panel which is academic research. Without good research it becomes impossible to make good policy.

I think that the interests of our little part of the world are sometimes forgotten. My guess is that most people would not be perhaps quite as concerned about what a researcher might do with their data as opposed to a business. Maybe they would be.

But I just wondered in terms of those who have done empirical research in particular in this area to the extent that it becomes more costly to do academic research obviously you get a lower supply of research, reducing the flow to policymakers.

I just wonder if those who have dealt with this could talk about what costs, if any, they have run into in trying to resolve the tension between privacy rules and academic research. How costly that may have been and any suggestions that any of you have for making that process work better?

MR. TURNER: Well, this project in my years of doing empirical economic analysis is unprecedented in terms of its magnitude and scope. Particularly because we were using 3.6 million actual credit files there were deep concerns about privacy laws and staying well within the parameters of the law.

For us to be able to append sociodemographic data on top of actual credit files was cumbersome because as you know the credit bureaus don't have the sociodemographic data and do not link them. It took legions of lawyers weeks of discussion to decide about how we would actually execute this and whether we could and under what conditions.

We finally figured out a method of doing this through a third party and washing all personal identifying information. What we got in terms of our output was so much code that we had to run through SAS. So we never saw any personal identifying information.

So, yes, the privacy rules do matter. They weigh heavily on research, and I would even suggest that our ability to obtain participation from firms who are involved in this industry. Obviously, if you’re analyzing credit scores in the credit industry you need participation from industry. You can’t do it without them.

But in fact some had fears that if they lent their models they didn't know what the outcome would be from the resulting analysis. If the outcome were suggestive of some privacy violations they would not be

three years ago.

We had been working since 1998 with one of the major bureaus who had basically taken credit report information and aggregated it down to specific geographic levels like county or ZIP code or whatever and then provided it for analytical purposes. It was on a large random sample of 30 million credit reports every quarter.

We worked with a developed product. It was showing a great deal of promise in terms of assessing credit trends across the country. The Federal Reserve Board was quite interested in it not only for safety and soundness monitoring but just for understanding how consumer credit was growing, et cetera. There were a lot of ancillary benefits associated with this product.

When Reg P was first promulgated there was initially uncertainty, but it wasn't FCRA considerations because all of these files had been stripped of personally identified information. However, there was the question of whether information was being used for a purpose other than for which it was initially collected and whether the bureau had to get consent from customers or consumers for permission to use it in these other ways.

The bureau actually suspended the product for research purposes for anybody that wasn’t using it to make a credit granting decision for about two years until that was clarified. It essentially put our project out of business and put on hold lots of other little research projects that have been undertaken or at least started with that product.

It has since been resolved. That product is now back in business, but for a two-year period it wasn't clear whether it was permissible or not. So all indications were that the regulators never intended for that to happen out of the regulation, but there is always sufficient vagueness when you pass these rules that you’re never quite sure what is going to result. So that’s one example where it impacted research.

MR. ZYWICKI: Peter?

MR. SWIRE: Going to back to HIPAA, medical data is very sensitive and confidential. Medical research is also a very, very good thing and we all want it to succeed. So there’s been a huge amount of work done on how do you do medical research consistent with confidentiality.

Under the HIPAA rule there’s three ways researchers can get data. One is they can deidentify, which is what you were talking about. The second is it can be with the permission of the individual data subject. The third is in the medical world they have IRBs, Institutional Review Boards, which are basically ethical boards to say yes, these researchers have promised to be very, very good and yes, the benefits of the research outweigh the costs and on balance we’re going to say go ahead with this.

That structure exists for medical research because of all the human subject data. That ability to let identified data be used for research, subject to some checks and balances, is something that could be extended beyond medical in the future.

MS. SINGLETON: Understand that even in the HIPAA context that there are sometimes problems with doctors discussing individual case reports at conferences because you can use the details of a rare individual case to trace back to an individual, at least in theory.

I’m not sure if academic research is so dear to my own heart. An area that I think is often overlooked that is dear to my own heart is the role that consumer information has in nonprofits because as you can see from the scratches on my hand, I’m a very active volunteer with the Society for Prevention of Cruelty to Animals.

There’s a tremendous amount of work that goes into just figuring out who we might possibly persuade to help us keep our sort of tiny little budget going a little bit longer. Direct-mail is a very im thek 202-833-8503

MR. ZYWICKI: Now, we're going to move on to our closing remarks of the day. We have with us Wayne Abernathy, the Assistant Secretary for Financial Institutions, Department of the Treasury who will talk about the use of information to fight identity theft. Secretary Abernathy.

SECRETARY ABERNATHY: Thank you for the privilege of visiting with you this afternoon. I am in a very unenviable position as all the good things have already been said today, I suspect. I'm probably all that stands between you and the exit door. So I will try to do my best to keep myself focused perhaps on some subjects that haven't been fully addressed today.

I have often been described as an economist, but down the road ahead of you often are for your good. I learned an awful lot; not enough to claim to be an economist, but enough to claim to be a consumer of economic information and economic presentations.

I want to talk to you today about what I believe to be the most significant problem facing consumers of economic products today: the problem of identity theft.

There are several reasons why I think that is the most significant problem facing consumers today. First of all, because they say it is. In a recent large, nationwide survey that was conducted of homeowners for the Fireman's Fund several questions were asked in addition to various insurance questions that the Fireman's Fund was really interested in. They asked the question have you ever been a victim of identity theft?

Interestingly, 12 percent responded that they had. Twenty-two percent responded that they knew somebody who had as in a family member or acquaintance or friend. Most interestingly, 90 percent feared, were concerned that

interested in. They asked the question ... likely were in danger of ... Tc(they were in danger of TD-yc worried that they might be candidates next. How does that affect the behavior of that 78 percent? I think it affects them profoundly. I think it affects the way they deal with economic transactions, financial transactions and particularly financial transactions where they are concerned that they might be excessively vulnerable to identity theft.

We find that particularly in the area of electronic commerce. We have today in the United States tremendous availability to electronic commerce. Something like 75 percent of all households now, I think, have a computer hooked up to the Internet either at home or some other place where there's easy access. Those numbers are constantly growing.

These people all shop on the Internet, kind of. They do what I would call electronic window shopping. They'll surf around. They'll look for a product. They'll compare. They'll focus in on the product and then they'll call the 800 number that's on the screen to engage in that transaction because they're concerned that if I fill out all that information on that screen and then hit that button that says send, I don't know where that's going. I don't know who's got access to it.

Businesses are doing the best to try to convince people that it's all encrypted and it's actually safer if you send it over the Internet than if you do it over the telephone. So far, we’re not having great success in helping people to believe that except in the area of discount brokers.

There not only are we convincing people but we’re giving people a very strong economic incentive to engage in your stock transaction over the Internet. In some cases you go from a $35 per trade transaction down to $8. In some cases, zero. People seem to be willing to take that chance.

Beyond that, we still have only somewhere in the neighborhood of 5 percent of economic transactions taking place over the Internet, yet 75 percent are window shopping.

That’s important because of the convenience to the consumer and the ability of the consumer to window shop and to look at a lot of different varieties of products at any one particular time when that consumer is comfortable at doing that, which is usually somewhere between 8:00 and 12:00 at night. But it’s also important because of the ability of the provider to connect with this particular consumer.

Let me give you an example of that very practical, what happened in my life. One of the consequences of the Gramm-Leach-Bliley Act was that I got a new car. I didn’t get a new car because I was passing the act. I got a new car because while I was working on the legislation, my wife was shopping for a new car. I came home and we got a new car. It was a good car, and I didn’t have the heart to tell her anything other than that.

It’s interesting because the day we actually got that car was a Saturday. Our bank isn’t open on Saturday. We finally made the choice though on a Saturday, and we said to the car dealer we like the car. We’ll take the car. We’ll be here on Monday to pick it up.

He said, why Monday? Why don’t you take it now? I said, well, we’ve already worked out our financing with our local credit union. We like the rate, we’re all set there. We’ve been approved, we just have to give them the amount. We have to tell them on Monday. They’ll cut the check and we’ll bring it to you.

The auto dealer said, that’s fine. Take the car now and bring us the check on Monday. Why could he do that? He could do that because he had access to a lot of information, and it was important to him that I made that decision while I was shopping and interested because statistics show that if I walked away from that dealer that Saturday chances went way down that I’d walk back on Monday.

Chances go up dramatically that I’ll be thinking about it. I'll be thinking, well, you know, maybe that isn't the right color. Are you sure we got the right price? Well, look at this, honey. This Saturday paper is advertising a car that's a lot cheaper than the other. Then we'd go shopping some more. It was important to that merchant that he make the sale when we're interested.

It was important to us too. We were happy because we could take that car right then and there. It simplified a whole lot of things, and we were happy consumers.

That can happen on the Internet with electronic commerce, and particularly financial services, if people will feel comfortable. But it's hard for people to feel comfortable with engaging in those transactions when close to a million people this year will be new victims to identity theft, when there are somewhere in the neighborhood of 11 to 12 million people who already number its ranks, and when the most virulent and difficult form of identity theft is the fastest growing.

That's not the case of identity theft where somebody takes your credit card and engages in a fraudulent transaction. That is the most common form of identity theft, but it is not the fastest growing. Because of a lot of work that has been done bfmkp eywiindustrf identity tran happirerce,,ing a cawhere in the

have to on our sensitive employees. And wow, it's just awful.

Maybe you'll be able to explain it. Maybe you'll be able to deal with it but that's when you first heard about it. Are these real? Are these real circumstances that happen? All the time. In fact, it was just driven home to my team that's been working on the identity theft issue. My lead staffer who's been working on this issue discovered just a few days ago that she'd been victimized by identity theft. Now she's trying to work her way out of the problem that she's been fighting a long time to deal with.

We at Treasury believe that this is the number one concern that needs to be addressed, and we're trying to address it in three ways. We think there are three aspects to this problem. All three of them need to be dealt with if we're going to get this risk of identity theft down to a level where people feel comfortable, more comfortable to engage in the kinds of transactions that are right there for them to engage in, that will improve their life and will increase the amount of commerce that's able to take place and decrease the costs of that commerce.

The three aspects that we want to deal with is we need to increase the deterrence. The first line of defense. What can we do to prevent the crime from even occurring or to stop the thief right in his tracks? Number one.

Recognizing that deterrence won’t be perfect, we’re also looking for increased tools that we can use to improve the chances of apprehending the identity thief. Thirdly, and perhaps most importantly, what can we do to reduce the amount of time it takes to restore the record, the credit history of the victim of identity theft?

As we began the process of gathering the information, the detailed information on fraud we came across countless cases of people who have taken years to restore their credit record. The GAO came up with an estimate that it is about 175 hours, man hours of work, to restore your credit record if you become a victim of identity theft. That is a whole month of eight hours a day, fi?pe060rove thtojr f timf woft.Ofss crse,te th a

acros(the caes of ladyht issbohhe)Tj/F1 1 Tf-14.8 (

thwasto illoigan the process orect rterinathit reco time.

We have got to address that and bring that time dramatically down. Now, what role does information have in dealing with that? I think we have to realize to begin with that identity theft is not caused by information. Identity theft is caused by lack of information. Let me put it this way. Identify theft is caused by information just as much as bank robberies are caused by putting money in banks. Now, it’s true it is much easier to rob the whole town when everybody puts their money in one place. You don't have to hit every single house in town in order to rob everybody if you can just find some way to get into that bank.

Now, banks have been robbed. Some banks have historically failed because they have been dramatically robbed. We have never thought that the policy in dealing with bank robbery is to eliminate banks. We have suggested that the way to deal with bank robbery is to improve the security measures. Improve the ability to apprehend the banking thieves and find ways to protect the depositor in the case of loss of funds due to robbery. We’ve got the FDIC in place. We’ve dealt with all three of those aspects.

order to engage in identity theft. He has to know something about the person he is trying to impersonate because he's trying to craft a mask. The identity thief child and where I met my wife. We moved down here because you can't find jobs in upstate New York, at least not in the town where we came from. So we moved to the Washington area.

Well, my wife was a little bit concerned that her mother was spending too much time mowing the lawn so she figured, let's buy dad a riding lawn mower. So we got dad a nice riding lawn mower and now we can't get him to stop mowing the lawn. Now, this year that's a good thing. The grass is growing as fast as he cuts it. He rides that riding lawn mower all around.

We bought that on a credit card from a place we have never been before, from a lawn and garden store located nearby where my in-laws live.

Very shortly after that purchase was made my wife got a phone call. Hello, this is the Visa fraud division. Did you make a significant purchase at a lawn and garden store in upstate New York? My wife was very pleased to get that call not because she was thinking well, why are you questioning me. She said, yes, I made that purchase and I'm glad somebody's watching and asking about that.

That's probably happened to many of you when you've taken your vacation to some place you haven't been before. You're checking out of the hotel and they might ask you this is a little bit odd of a transaction. Is this really you? And then they try to verify that it's really you.

Now, the big credit card companies can do that my customer and I can compete with the big guys and I can give him additional choices.

Today you can do that because the information is shared all across the country in a uniform, standardized way. I can find out whether that person is legitimate or not. We can prevent the crime right there.

But how about if a crime has actually occurred and I'm a law enforcement officer. What does my staffer do who has now been victimized by identity theft? Where does she go? Does she go to the Montgomery County Police? Does she say, well, you know I've been victimized by identity theft. Well, where did this happen? Well, it was on my local department store card.

Well, is this a national department store? Well, yes it was. Oh, but the charge took place locally? Well, no, actually it took place in Illinois. Oh, well, let me give you the name and number of the police department in Illinois so you can get in touch with them because that's where the crime took place.

Contact the people in Illinois. Well, this crime took place there. Well, how do you know about it? Well, I found out about it here in Montgomery County. Well, that's in Montgomery County. How do we cooperate? How do we communicate with one another? How do you get all that information together?

Unless you have a standardized system of information sharing, how do you get the information to all the different law enforcement venues that identity theft has occurred and has occurred in the name of so and so? People ought to be on the lookout for it and can we amass the different data points that might be occurring around the country, because many of these identity thieves are getting pretty smart and they hide behind the different state boundaries to try to get away from their crime.

How can you put all those pieces together? You can do it with the information that's available today in the uniform sharing of information as well as other systems that are in place using this wide national sharing of information.

Then, of course, the third point is if you've been victimized and it isn't the type of victimization by somebody you know, it's somebody you don't know. It's happened in who knows how many different places, how do you know where it's all happening? How do you get the word out to everybody, I'm not the person who had this account headquartered in Peoria. I'm located here in the Washington, D.C. area.

Unless you can instantaneously send out the information put an alert on all your credit records, watch for anybody who's trying to open up a new account in my

But all of these solutions rely upon the use of information to fight identity theft rather than putting in place new barriers to the movement of information. As you put in place these barriers to the use of information you create shadows. Remember the identity thief operates where there's lack of information. He operates in the shadows. When you erect shadows you create opportunities for deception to occur.

We appreciate those of you who have given us your best ideas. In the next few weeks we hope to be presenting to you what we think are the ideas that make the most sense in a comprehensive way. Then we'll appreciate your comments about whether we have it right or not. We are committed to fighting this crime. We're committed to using the tools that are available to us. Where changes in the law are valuable in this fight, we'll be asking about those changes.

Thank you for this opportunity to discuss this with you and most especially thank you for the help that you'll lend to us in the future as we continue to fight this challenge.

MR. ZYWICKI: Thank you Secretary Abernathy.

(Applause.)

MR. ZYWICKI: I want to say thank you to everybody who's come today. It's been a long and full and fascinating day and I thank you all for coming.

(Whereupon, the hearing concluded at 5:15 p.m.)

CERTIFICATE OF REPORTER

I, Deborah Turner, CVR, do hereby certify that the foregoing proceedings were electronically recorded by me via audiotape and reduced to typewriting under my supervision; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were transcribed; that I am not a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome in the action.

DEBORAH TURNER, CVR

My commission expires: 02/01/2006