THE BROOKINGS INSTITUTION

ONLINE IDENTITY AND CONSUMER TRUST

Washington, D.C.

Tuesday, January 11, 2011

PARTICIPANTS:

Moderator:

DARRELL WEST
Vice President and Director, Governance Studies
The Brookings Institution

Panelists:

ED FELTEN
Chief Technology Officer
U.S. Federal Trade Commission

PATRICK CROWLEY
Professor
University of Washington, St. Louis

ALLAN FRIEDMAN
Fellow and Research Director, Center for
Technology Innovation
The Brookings Institution

* * * * *

P R O C E E D I N G S

MR. WEST: Good morning. I'm Darrell West, vice president of Governance Studies and director of our Center for Technology Innovation at Brookings, and I'd like to welcome you to this forum regarding online identity and consumer trust.

As the Internet evolves, new threats to personal information are emerging. This includes issues such as session hijacking, history sniffing, cross-site profiling and phishing. Many of these attacks are technical in nature and not easily understood by consumers, others are of a more garden variety.

Just last week I was on a social media site and I received a frantic chat message from a friend of mine who said he was in London, he had just lost his wallet, he had two hours to make some event and needed cash right away, kind of a classic example of his social media site having been hijacked by evildoers.

So this and other types of examples suggest the need to think about ways to maintain online identity and build consumer trust in the Internet world. Today we are releasing a paper on online identity, it looks at threats to identity and ways to think about the subject. As we will discuss in a moment, we make a number of recommendations to protect digital identity. To help us understand issues related to online identity, we have brought together a number of distinguished speakers.

Allan Friedman is a fellow in Governance Studies and research director at our Center for Technology Innovation. He has a B.A. in computer science from Swarthmore College and a Ph.D. in public policy from Harvard. His areas of interest include privacy and security in the online world and electronic commerce.

Patrick Crowley is professor of computer science and engineering at Washington University in St. Louis. He works in the Applied Research Laboratory there. His interests span several areas of computer and networking systems. He has expertise in multi-core processors and memory systems, programmable network routers and building novel networks using programmable network routers. He's very knowledgeable about security issues.

Ed Felten is chief technology officer for the Federal Trade Commission, which he joined quite recently. In fact, Ed just told us today officially is his second day on the job, so that's literally hot off the press, although he has been working with the Federal Trade Commission earlier. Previously he was a professor of computer science and public affairs at Princeton University, he served as a founding director of the Center for Information and Technology Policy there. He has been a consultant to several federal agencies and departments and has testified before

Congress on issues of technology, computer security and privacy.

So I’m going to start with Allan today. We put out a paper on online identity and consumer trust assessing online risk. Can you give us a short summary of the highlights of this paper?

MR. FRIEDMAN: Sure. So why is identity important online? And the report argues that the identity is the means that an individual has of establishing a relationship with an online system. So identity is the very core of the relationship for online trust. And we talk about many different of the technical components of what establishes an identity, but essentially it’s how do you prove who you are to a system.

Now, in the context of fraud, I don’t usually like the term “identity theft.” When we think of theft, we think of an attacker and a victim, and if we want to deter theft, we basically argue that the defender should -- the victims should defend themselves more. In many cases, what we called the fraud, in fact, it’s impersonation, someone is coming up and saying that’s my money in the bank when, in fact, it doesn’t belong to that person.

In the case of online identity fraud, I would argue that theft is a reasonable way of thinking about it, because we have a very small set of means of establishing relationships, it’s the online credentials, and so the risk here is there are a myriad of ways that an attacker can compromise the online credentials.

And we in the report lay out a number of different vectors that use different aspects of the system. Attacker could be listening on a local wireless network and simply obtain the cookie the way that the online system recognizes your computer automatically, they can steal the password through phishing, as we've talked about, there are a number of different aspects that the report talks about.

The challenge in addressing these issues is that we have many different actors at different layers of the system of thinking about identity, and it is a coordination problem between the online services, the vectors of the attack, which often are not part of the transaction, if it's a local network or a public wireless network, and the web services that are responsible for authenticating the user, and the users themselves, who may or may not be aware that an attack is even going on. So it's not purely technical, nor is it purely policy.

We highlight three large areas for thinking about a solution. One of them is thinking about the identity platform. And on Friday, Secretary of Commerce and the cyber czar in a speech in California sort of reaffirmed the national draft -- the draft of the national strategy for trusted Internet -- trusted identity in cyberspace.

And first it's important to know a number of the press reports have said this is about Internet and driver's license, it's very much not that, it's about rethinking the ecosystem of identity. Instead of having a one to one relationship, where everyone has a unique relationship with a single web server, is a way of having identity providers and having various web services rely on different identity providers to establish identity. I'll be happy to talk about that more later.

There's also something that the FTC has done for financial fraud using identity, which is the red flag model, that essentially anyone who uses identity information in a creditor relationship, that is, not just financial services, but also anyone who is providing a service now and billing for it later, needs to look out for identity fraud red flags, have an internal system and monitor them. Now, this is an important approach because it's contact specific. Every business has to develop their own way of doing things that reflects their own identity infrastructure, their own value at risk and have a plan in place.

Now, what's interesting mapping this to the online model is, one, many of the sites aren't in this relationship. So of the top five targets for phishing attacks online, according to some spam metrics, three of them don't fit this classic creditor model, yet they're clearly attractive targets for fraud.

So what should we do? We should have these services perhaps be under a similar regulation, either voluntarily or mandatorily. Now, what's interesting is we talked in the report about online tracking as a threat to online identity, and many of these sites also have very specific internal tracking mechanisms. And the report argues that if you have a very sophisticated tracking model, that it makes sense that you should have the ability to have a fairly sophisticated model for monitoring fraud and a much more advanced red flag approach, and this allows the defense to scale with the complexity of the system.

Finally, the report argues the importance of usability. Now, just a few notes on this. It does take some time to train users. Users are now more sophisticated; the attackers have understood this and have changed their habits in time. And it's very important to think about how long it takes new solutions to diffuse through the user space, especially if we're talking about something that's going to go on the user machine.

People, unfortunately, do not update their software as fast as the engineers would like them to. So we need to understand that the user is often a weak link in this, and how do we enable the user to make choices without overloading them with information and at the same time giving them no choice in the matter. That's all, thanks.

MR. WEST: Okay, thank you very much. Patrick, you are an expert on computer security, give us your perspective on this.

MR. CROWLEY: Yes, in thinking through my comments this morning, I thought it might be helpful to emphasize and, in some respects, amplify aspects of this report that we've put together. Digital identity in its full extent, for me, is a canonical example of a cross-cutting issue. And as a technologist, I've seen in my own work how, considering the implications of trouble with digital identity through a purely technical point of view, is risky.

In my work, I've been the originator of some of the most successful methods for network security, particularly in a domain known as deep packet inspection, and in my work, my students and staff and I put together what we knew to be the most successful methods known. And in talking with the people that I consider to be the most important consumers of this type of technology, the government agencies and corporations that most need to protect their critical information, they were operating under the assumption that they had already deployed this type of technology in their operational networks.

And what became clear to me is that there was an enormous gap in understanding between what technology solution providers were carefully describing in their product descriptions and what the ultimate end consumers were really getting in the systems that they purchased. So this, to me, was an obvious and enormous risk. And in particular, with my work with the federal government, it became apparent that the federal government was spending enormous amounts of money on technology that wasn’t doing the job that they thought it was doing.

So this brought into sharp contrast for me the need for technologists and people interested and responsible for policy matters to engage more meaningfully on the subject, and this is why I’m here today. That’s why I left my lab and flew to Washington, D.C., to chat with you here today.

I wanted to very briefly just touch on two themes that I think are present in the report, but bear some further elaboration. The first has to do with what we can expect from technology in the future as it relates to digital identity. And the news, in my opinion, is not particularly good. I think that the risks and the dangers in the future are far greater than they are today. And I don’t mention this as a scare tactic, I mean this in an objective sense.

And one concrete illustration of what I mean can be seen in, I believe it’s Las Vegas right now, where the Consumer Electronics show is underway. The high-level bit for all of consumer electronics today is that it’s all Internet-enabled and you can do extraordinary things. You can link your television with your Facebook account, and so that’s an unusual coupling between your digital identity and consumer electronics.

And I’ve seen in some operational networks that I help to keep safe, I’ve seen the consequences of Internet accessible consumer electronics be exploited by malicious actors, things that we wouldn’t typically think about. You go to a store and you buy a new printer, you bring it home and you attach it to your home network. Most of us would be surprised that there’s a web server on that printer that has default user names and passwords, and it can act as a little storage server or a little e-mail server. It’s an unusual sort of thing.

We don’t think of our consumer electronics as having that sort of character, but they certainly do. And all of our employer networks, if you’re at a university or a government lab, there are at any given point in time hundreds of devices that have been plugged into the network that can be exploited through typically what is some sort of default of digital identity, some account that’s just sitting there that hasn’t been properly manned.

Finally, I wanted to emphasize the second theme, which is the relationship between innovation policy and, you know, ultimately security. This is a broad point, one that I think all of us probably understand, but it does bear repeating.

The process of innovation, so creating a new technology that has meaning and has use, but doesn’t yet exist, is a valuable process and it's one that's very difficult to get ready. And I think it's widely recognized that regulation and heavy requirements can unintentionally hinder that delicate process. And so that's the real -- that's a great danger in trying to qualitatively improve the health of information security broadly.

If you, in a well-intentioned way, create strong regulations that increase the cost of innovating, you may or may not improve the health of information security, but you will certainly increase the cost and diminish the likelihood of meaningful innovation.

So this fact, coupled with what I would consider to be an unhealthy posture in the information security industries, so what I mean by unhealthy posture is the fact that necessarily you can imagine that companies that are in the business of selling you security solutions, they have incentives built into their DNA to help you understand just how scared you ought to be in order to derive maximum benefit from the product or service that they offer. I don't have a solution to this particular question, but it is -- I think largely it's a problem -- it's a self-defeating dynamic in that industry, and therefore, I've more or less come to the conclusion that I don't know yet who will make a meaningful impact on our information security posture, but I'm pretty sure it won't be today's information security industries. I think that they're self-defeating in many respects.

And for Darrell, something that we can perhaps talk about a little more in the Q&A session, for a lot of people who are casual computer users, the issues surrounding digital identity seem like they can really be solved through proper use of tools like encryption. It's simply a matter if we encrypt everything, then everything should be okay. It turns out that encryption both helps and hinders, and I consider that to be a very interesting point of discussion, which if there's interest, we can return to later.

MR. WEST: Yeah, we will definitely come back to that. Ed, you expand both academic research and now public service, so what do you think we should be focusing on, what are our tough challenges?

MR. FELTEN: Well, first let me react a little bit to the report. I think the report does a nice job of highlighting the problem of identity and mapping out the space of issues that we need to deal with in looking at identity.

Sometimes it feels like in computer security and privacy space, we're often looking at the same issues from different angles, and one of the important angles from which to look at these issues is the angle of identity. And you see that in the report discussion of issues, which might look one way if viewed from a different angle, but viewed to the angle of identity, you get I think a useful and important viewpoint on the space.

Certainly when you're talking about identity and practice, identity online sometimes plays out in a different way than it does in physical space. In physical space we tend to talk about and think about identity as being a sort of strong mapping of from a body who's here in front of us to some notion of identity, name, Social Security number, registration in some database. But online, there are more shades of identity with which we are often dealing. Sometimes an identity really is mapped strongly to a single individual, to that real world identity. But sometimes when we're talking about identity online, what we're really talking about is knowing that this is the same person who we saw before, without even knowing who they are.

On a lot of sites, that's really what the authentication of a user is about, it's knowing that this is the same person who set up the account before, even if we don't know who they are, and sometimes that's just what you want in order to make a service work. You want this person's friends or peers or counterparties to know that this is not -- that this is the same person who they dealt with before.

Sometimes when we talk about identity, we're not really talking about knowing who the person is or even that they are the same person as before, but we're talking about assembling a kind of profile of information about them. There's discussion of the online tracking issue in the report, for example, and often that's what the issue is. Really the concern that people have is of someone assembling information that is particular to them and personal even if that party doesn't know precisely who they are in the real world.

Now, as you move down that scale from strong, binding to a real identity, toward just having information about the person, it becomes easier to do with confidence, it becomes easier to build the technology with confidence.

It's very difficult online to map an online identity to a real world identity simply because you don't have many building blocks with which to do it. And the cost of connecting to a real world credential, for example, to actually seeing someone's past or some strong ID is difficult.

So online more often dealing with the weak identity, weaker notion of identity, and that has its pros and cons. We often talk about the cons of a weaker identity, but it's worth recognizing the advantages of it, as well, that if we are dealing with a weak identity, and we don't make the mistake of relying on it as if it were a strong identity, then we can often end up with a system that's relatively resilient.

Finally, I wanted to talk a little bit about the role of coordination problems in this space, something that really occurs throughout the security space. And there's discussion in the report about the role of encryption, and I'm eager for this discussion about pros and cons of encryption.

But certainly we've seen in recent times examples of security attacks or exploits that take advantage of a lack of encryption settings. So, for example, the fire sheet demonstration which showed ways of hijacking people's identity.

So the basic back story is, if you go to scenarios, if you're in a coffee shop on some kind of open Wi-Fi network and you're using a popular site which doesn't encrypt their sessions, but a site to which you're logged in, then someone who's present in the coffee shop on that Wi-Fi network can capture a cookie which represents your identity and then impersonate you to the site.

The fix for this is to make more use of encryption. And there's a whole story about why that hasn't been the case yet. Some companies are certainly ahead of others in implementing this encryption, but it's an example of a case where some engineering effort could provide a measurable benefit to end users. But I'm eager for the discussion up here and with the audience.

MR. WEST: Okay. Both Patrick and Ed mentioned this issue of encryption, so why don't we jump into that? Patrick, you were noting there are ways in which encryption both helps, but also hinders, so what is your view of encryption as a way to help assure user identity?

MR. CROWLEY: Absolutely. So clearly encryption plays a fundamental role in keeping identities secure. The specific thought I had in mind when I mentioned how it can hinder requires a little bit of background description, and it relates to how organizations attempt to keep their networks secure.

So when you are at work, your office PC or laptop has, in all likelihood, anti-virus software installed on it for the expressed purpose of keeping your machine safe in case you, one way or another, get malicious content into your e-mail inbox or into a file folder on your hard drive.

It turns out for medium- and large-sized organizations, it’s difficult to ensure that every device on the network has such software installed. And so as a complimentary security solution, most medium to large scale organizations use a class of networking system called an intrusion detection system, and these systems largely operate at the point that your organization connects to the Internet, and its role is to examine the traffic as it comes from the Internet into the organization or sometimes to check for content leakage and sometimes examines data going in the other direction, as well.

But in principal, an intrusion detection system operates just like your anti-virus software package. It looks at the traffic, looks inside the bits in the packets and decides whether or not there's anything bad inside those packets.

It's a -- I think such systems are widely recognized to be distasteful solutions for a number of reasons, not the one you're thinking. You're probably thinking this is an invasion of your privacy. Most people in security don't mind that at all. It's distasteful from a technical elegance perspective. In order to look inside these packets, engineers and architects have to ignore the explicit layering of information that helps keep the system orderly in the first place.

So the way encryption causes a problem here is if you, as a user, happen to use Gmail for your personal web mail service. Well, your access to Gmail is encrypted, so that's a service that, for most people now, is accessed through the secure variant of the HTTP protocol, and the consequence of that is the intrusion prevention system that your employer operates cannot look inside the bits of your Internet packets to see if anything dangerous is going on there. And many of us would be very surprised to learn just how widespread the use of these intrusion prevention and detection systems are and how completely useless they are rendered through end-to-end encryption.

And so encryption in this way really does cut both ways. It can help secure the authentication step, but it can also obscure the perspective that network securities, administrators have in keeping networks safe.

MR. WEST: Ed.

MR. FELTEN: Sure, let me -- yeah, let me expand on that a little bit. One of the trends in technology recently has been toward having a sort of -- having the physical structure of a network differ from the logical structure, if you will.

So, for example, if I were to open up my laptop here and go to read my e-mail at the FTC, I am physically here at Brookings, connected to the network through some -- presumably through some Brookings connection or maybe through my cellular carrier, but I’m logically inside the FTC network. An encryption can build me a bridge from here to there so that I am effectively -- I’m in the same security posture as if I were sitting at my desk in the FTC. So encryption can give me that, but then once I’ve gone there, then the intrusion detection that goes on on behalf of not only the agency, but the taxpayers, to make sure I’m not doing things I shouldn’t be doing, will still operate.

And I think increasingly, as people move around and start to connect to the net through all kinds of devices which are physically eaves droppable or start to connect from a lot more places, I think you’re going to see a lot more use of encryption, but it’s not necessarily at odds with doing appropriate intrusion detection or appropriate scanning of network traffic.

A lot of the hard decisions come in deciding what information should be available to inspection and scanning by whom. I think once you have a clear answer as to what should be scanable by who, then, generally speaking, encryption can be used to make that possible while protecting against other undesired intrusion.

MR. WEST: So just as a follow-up point, wouldn’t you agree, though, that your employer, the FTC, in this instance, does require a certain transparency in the network traffic that you participate in when you’re logically connected to that network, and so that might result in network access policy such as you cannot check your Gmail account from work because the FTC wouldn’t be in a position to verify that you’re accessing information, secure information across that wing?

MR. FELTEN: Sure, and that’s certainly the kind of decision that a network administrator there would be making.

MR. WEST: Right. Allan, what are your views in terms of policy priorities, what we should be focusing on?

MR. FRIEDMAN: So when I think about how do we prioritize, sort of follow the economist principals, where is it cheapest, where is the bottleneck, who is actually in control and sees the most information, and from that perspective, rather than focusing on a distributed user population, it makes sense to concentrate on the authenticating party.

So in financial fraud, it makes sense to say maybe my bank should bear a decent role and responsibility of making sure it doesn't accidentally give my money to someone else. And similarly, in the online space, we need to have better tools and faster tools to sort of be aware and detect what's going on. There are some fairly low hanging fruits that can happen. One of the papers I cite in the report by a Berkeley team on the use of http only cookies, which is the idea that really it makes sense, your session cookies should really only be able to be set by the web server that you're talking to and be read by the server that you're talking to. And if another server wants to actually read it, you should have some prevention for that to take place, so we can sort of promote this as a policy to come out and encourage organizations to do this.

Now, how do we do that without imposing too great a cost on a very innovative and dynamic ecosystem? Well, part of it is that cost has been there all along, it just hasn't been on the books. It's a classic case of inexternality. It's the equivalent of a company that is polluting a lot and then complaining about the cost of cleaning up the pollution. This is risk that has been part of the ecosystem and we're only now realizing it and trying to put it on book.

But I think from a policy perspective, coordination and standards are key in driving down costs. How do we get the different actors to work together for maximum efficacy, and how can we do it so that there are fairly easy turn key solutions, and that is a role that the government can play a role in.

The Department of Commerce has recently sort of announced that it is going to occupy that role in a number of different areas in information security through NIST. And certainly the FTC, by promoting fair information practices that are updated to a more web 2.0 environment, can also play that role.

MR. WEST: Several of you have mentioned this tension between innovation, on the one hand, versus a regulation on the other. You know, we want to encourage innovation, there are, you know, exciting, new applications that are coming along, but then, on the other hand, there is some need either for either self-regulation or perhaps more firm regulation. How do we get that balance right, so that we maintain innovation while also protecting consumers and users?

MR. FELTEN: Let me jump in. Well, one of the things we can do is to -- one of the things that government can do is to act when users have been harmed by overly careless behavior by industry, and that's one of the roles that the FTC has played in its enforcement role. And, obviously, if you take that too far, and if it becomes an exercise in hindsight as opposed to -- purely an exercise in hindsight, that's not going to be helpful. But certainly, to the extent that companies are inappropriately careless, that is something that will I think get attention.

Rather than making rules, detailed rules in advance that things should be done this way or that way, which often does have this one size fits all problem, the amount of -- the strength of an identity, the amount of protection that's needed is really going to depend on the nature of the use.

Some of the uses of accounts and passwords online really have very, very little at stake. In fact, often -- sometimes those uses are not even for the protection of the user at all, but simply a way for a publisher, for example, to have a better idea of which users are reading which articles.

So certainly the appropriate level of care is going to differ a lot, but I think there is a role for government to act when a company has been inappropriately careless.

MR. WEST: Allen.

MR. FRIEDMAN: So going back to the red flags model, I think that is the advantage of being appropriate and specific to a company's business model. And one is the case that as a new idea grows and rapidly becomes adopted, then it will be more likely to draw the attention of an organization like the FTC, focusing on the risk of consumer harms rather than blanket precepts, but also, it should be specific to that organization.

Now, organization specific regulations sometimes can be very onerous. On one hand, I think security experts in the room will agree that security is a process, it is not a single tool, but focusing on the process, if done poorly, is just basically the equivalent of writing checks to consultants rather than actually creating things. It's a culture of compliance rather than a culture of security.

So that is something to be very careful of because that -- you're imposing lots of costs on established players, you're not really helping to promote innovation, you're just imposing cost across the system. So we need to be very careful as we come up with these process approaches. However, I think the process approach is preferable to a blanket regulation.

MR. WEST: Patrick, you mentioned the danger of heavy regulation, so what are you worried about on this front?

MR. CROWLEY: So the big concern has to do with raising the costs for a small group of smart, hard working innovative people to create something new that the rest of the world complain with. So the IT innovation right now has the extraordinary advantage, and always has had the extraordinary advantage of being relatively inexpensive.

So a small number of people can raise a very modest amount of funding, they go to market with a great idea to see if it works. If you consider the similar amount of -- or the equivalent amount of investment that would be required to take it, a medical device company or any other biotech related company, there the regulatory and legal burdens are much, much greater, therefore, the capital requirements are much greater, too.

We certainly don't want that to happen to IT. If you can somehow account for all of the costs, the costs for doing so would dramatically outweigh -- well, the benefits lost would dramatically outweigh the costs of even implementing a program like that. The other thought that I wanted to mention with respect to what can really be done, what happens in the world today right now when there are data breaches of any kind, whenever a large service or a large employer experiences a loss of information, or even a suspected loss of information, most enterprises and universities have the practice of disclosing, at least to their employees, exactly what's happened, and that's very, very healthy.

Certainly we'd all want to know this from our employers, but you might also imagine that for service providers, if some popular networking service experienced a data breach and had to come clean about that publicly, there may not be a fine from the government involved, but there has surely been a high price paid because certainly users will think twice about disclosing further information to a company that has had a data breach.

So the way things are operating now seems, to me, like a reasonable balance. It is completely reactionary, of course, it’s -- the public disclosure of data breaches is something that, in most industries, is not something that’s actually legally mandated, but it is done as a best practice willingly on the part of the enterprise.

MR. WEST: Ed, should we require more disclosure on the part of the service providers for these types of data breaches?

MR. FELTEN: Well, with respect to data breaches, there are already laws that make disclosure mandatory in some cases. And that has really led to a change actually in the -- I think in the way that consumers see these issues. The laws requiring breaches have led to more notifications, which have led consumers I think to get a more accurate picture of how often breaches actually do happen, and also have led companies to -- have given companies a stronger incentive to avoid breaches, so certainly that has been a positive thing. As to whether we need more or different law in that area, I'll leave that to smarter people. But I think the law we have has been helpful.

MR. FRIEDMAN: So one thing we know about data breach reporting is that certainly public reports of breaches applied to publicly traded companies has gone down, and the publicly reported breaches from government agencies, hospitals and schools has gone up. Now, the latter increases, probably because we have better reporting mechanisms, it is an open question as to whether the decrease in reports from publicly traded companies is a function of better market incentives or if they've actually sort of changed their reporting requirements to have them go down; I certainly hope it's not the latter.

One interesting component on data breaches of web services is, there is some real harm here. So when the blog empire, as the Gawker empire was attacked and its password file was released, we learned two things.

One, we learned that Gawker didn't do a very good job of protecting their passwords. There's an important step that they didn't do to protect the password file, which meant that they were very easily recoverable.

But, two, many websites actually said we're able to identify users of their own website in this database because there's a common identifier. And they were notified and said, listen, we think there's a reasonable chance you reuse your passwords because that's what users do, they reuse passwords. And if it's an important enough issue, then a compromise of the credentials on one website can lead to an attack on another website. And several important web servers actually temporarily disable their account and force them to do the password recovery mechanism.

MR. FELTEN: There are -- this is one example of how market failure can happen in this space, right, where an error by one company, by one provider, can have effect on others. Another example is, if a breach happens, and it's not detected, users may be harmed and not know how it happened.

Some of you have probably had this experience, where charges start showing up on your credit card that aren't yours consistently, something happened to cause that. You may not know and you may never know who was at fault, whose error allowed that to happen. And to the extent that the party that made the error isn't -- that isn't detected and they don't suffer some consequence, that also is -- that also can be a market failure.

MR. FRIEDMAN: On that point, going back to the organizational side, I would argue that PCI, the payment card industry's set of standards that have been voluntary, but have been pushed because of contract agreements, so that certain banks won't work with certain other players in the payment card infrastructure, and a bunch of people that interact when you use your credit card has actually I think done a decent job. Compliance does lead to great security. Now, it's also important to know that this doesn't make -- it doesn't mean that the credit card infrastructure is now secure, it's very much not, and there are -- there have been publicized breaches by firms that have been judged to be compliant. And there are two things we learn from that: one, there's more to do, but also, we shouldn't let the perfect be the enemy of the good. We're all better off because of the PCI standards.

PCI standards were not cheap to implement, they were done private sector, self-regulation, but I think they do make a difference even if not a perfect --

MR. WEST: Let me ask one last question and then we'll open the floor to questions and comments from you. The recent announcements about identity strategy have insisted that a robust identity platform can actually increase privacy online, how would that work?

MR. FRIEDMAN: So one of the important things to think, and Ed really highlighted this aspect, is that identity doesn't necessarily mean the entity, it doesn't mean all of me, it can be a single feature. And so in the offline world, friends from Europe are often shocked that they're asked to show their identity papers when they enter an establishment that serves alcohol so that they can drink, and showing papers is a big deal. Really the only thing that a bar needs to know is, is it legal for me to drink. It doesn't even need to know my age. It just needs to know, yes or no, one single question, can this person be served.

And it's very hard to -- you know, we can't just have a token that each of us can carry around in the real world. Online we can. It is very easy to come up with secure credentials using cryptography that someone else will verify a certain part of our identity that we can then pass on to some web service.

It doesn't need to be me, it doesn't need to be tied to all of my other online identity information, it just needs to have a single piece of information that is relevant to the transaction. What state do I live in, what is my shipping address, what is my previous history with this website, all of those things can be divorced and sent as a case-by-case basis.

MR. FELTEN: Just to amplify that a little bit, in cases where the goal is really to authenticate that this is the same person who was here before, you, again, don't need to know who that individual was, nor do you necessarily need to know that this is the same person who was over there before. By using cryptography appropriately in an online setting, you can really divorce those different aspects of identity from each other in a strong way.

Currently, you can do that in a password based system up to a point. In principal, you could choose a different user name, an entirely different password on every site, but I doubt there is a single person in this room who does that everywhere they go.

MR. WEST: I promised I'd open the floor, but I just have one follow-up question on that. Do you think passwords will be the primary device for security in the future or are we going to move to some post password approach? Anyone.

MR. FRIEDMAN: I think certainly in the longer run, we're likely to get beyond passwords as the primary identifier. One of the biggest problems with passwords is that they're subject to -- first of all, people have to remember them. You have relationships with so many different parties that it's not realistic to have a separate password for each site which you will remember; nobody's memory is that good, number one. Number two is that passwords are inherently subject to guessing attacks, and guessing attacks are computational in nature. Guessing attack searches over a range of possible passwords. And as computers get faster year after year, the number of possible passwords that can be searched by an attacker is always growing, which means that our passwords have to get progressively harder and harder and harder to remember as time goes on, and we’re not getting that much better at remembering this information.

So the thin margin between what we can remember, on the one hand, and what a computer -- an attacker can guess is just getting narrower and narrower. Something has to give at some point.

MR. WEST: Patrick.

MR. CROWLEY: Yeah, I was just going to say, I think Ed is dead on there. Of course, the great virtue of passwords is that they’re cheap and easy to create, and for that reason, I think that passwords will always be with us, but I do think that alternate mechanisms will come to play for those accounts that can actually bear the cost of doing so. So, for example, in our financial services accounts, I think that there may be stronger mechanisms that are used, but for the vast majority of our web services that really touch on our casual online identities, passwords are likely to be the thing for the foreseeable future.

MR. FRIEDMAN: I also believe in the long-term existence of the password, if not its successful use. I think we’re going to have them for a couple reasons. One, the mechanisms that you talked about, you know, people have for their companies a small file that generates a secure key, this works well for your employer because -- one employer or several employers, it does not work well for financial institutions, because, again, you have this one to one relationship.

So before we move into that model, we're going to need a layer of identity infrastructure, which is something that was in the commerce report. It's going to be a while until we get there. One solution is to have fewer passwords. So, you know, you still use passwords, but now you just have one or two for different identity providers.

Another approach is to use the device itself as part of the authentication system. And as chip manufacturers are starting to build trust into the base of the chip and have that filter up so that it's less vulnerable to phishing attempts and to exploiting users and have malware interject bad values, there are some -- there is some evidence of this, but again, it's going to require an infrastructure to use.

MR. FELTEN: In the security world, we talk about three different ways of authenticating a person. We either authenticate something you know, that's a password; something you have, that's one of these little fobs that gives you a number or something; or something you are, that is some physical aspect of your body like your fingerprint, and those are really the only three possibilities. We'll have to use one of those or some combination of them going forward.

MR. WEST: The last time I counted, I had more than 60 different passwords, so I can actually remember my passwords, but I can never remember which password goes with which particular feature.

But let's open the floor to questions and comments from you. Just raise your hand. We have someone with the microphone. We have a couple questions up here, up front. If you could give us your name and your organization, that would help us, as well.

MR. MORCOM: Thank you. Do I need to stand up?

MR. WEST: Your choice.

MR. MORCOM: Ty Morcom with Oracle. Most of what we talked about was malicious acts in terms of hijacking identities. There's a whole cottage industry around legitimate data aggregators, which the onus of responsibility to get your record removed moves to the user. So now you're talking a multi to one relationship. I have to communicate with each of the 10 that I know of, there might be 30, to get my name off of their list.

Where do you see government regulation and FTC potentially in terms of having a Do Not Share equivalent of the do not call that was put in place, or at least educating the consumer? Because right now that burden of removal is really all, and even then it's not comprehensive because more companies pop up faster than I can write letters and copies of my driver's license. Thank you.

MR. FELTEN: I guess I should respond to that one first.

Certainly the issue you highlight is an important one, that it is more difficult to deal with these issues in a case where the consumer does not have a direct relationship with the party who is gathering or using the data. In the case where there's a direct relationship, it's easier to structure protections on top of that relationship. And you can view the use -- gathering and use of information as something that might be negotiated between the user and the other party with whom you're doing business. But in the case of a third party who doesn't have that direct relationship, it's more difficult.

This is an issue that was discussed at some length in the FTC's recent draft of the privacy report. And in particular, you talked about the do not call list, the analogy to do not call. One of the things that was -- that's in the FTC privacy report is a discussion of Do Not Track mechanism for the web.

And this is an issue that is still under discussion and one on which we are looking for comments from the public. But the basic outline is to give consumers a way of acting out of -- of opting out of online tracking in the behavioral advertising or other setting in a way that is relatively straight forward for consumers to understand and exercise.

MR. MORCOM: And so this goes a little bit beyond Do Not Share, as well, right?

MR. FELTEN: Do Not Share, yes.

MR. MORCOM: So it's going -- goes to multiple (inaudible). It has nothing to do with how (inaudible).

MR. CROWLEY: It can form a composite of -- a composite sketch when that aggregator pulls (inaudible).

MR. FELTEN: Certainly right. I don't want to generalized too far here, because there are certainly restrictions on sharing in some cases, depending on what the relationship with the consumer is, what promises have been made and so on.

There's not a direct discussion of a Do Not Share mechanism in the FTC report. There are some complicated issues about how to look at restrictions or limitations on collection versus use versus sharing, but a Do Not Share mechanism is not something that has been directly proposed at this point.

MR. WEST: You had a question?

MR. DELBIANCO: Hi, Steve DelBianco with NetChoice. Allan, you said earlier in your report, on page 12, talks about tracking cookies, and you mentioned these tracking mechanisms are exactly what's needed to detect irregular activities. And then Ed Felten also talked a little bit on tracking cookies as being a weaker shade of identity in the sense that, you know, it's a person, but you don't know who the person is. But I would offer a different perspective than tracking cookies.

Most tracking cookies don’t actually have the identity of the person, the ID and password in it. They just identify a browser instance on a given machine, that’s it. It doesn’t really know whether it’s the same person who’s visiting that browser on that machine or not. So in that respect, it’s even weaker than person. It’s so weak as to only be -- I know I’ve seen this browser on this machine before. And if the reliance on these tracking cookies were to be of some assistance, as you say on page 12, that might clash with the Do Not Track option that’s widely mandated in industry where consumers won’t be allowed -- or sorry, consumers will be encouraged to take the Do Not Track opt-out option and cookies will not be able to be used for the mechanisms you anticipate.

MR. FRIEDMAN: I think you’re exactly right, this is a complex space where pushing down on one thing makes something a little harder. But there are a couple of issues here, so, one, you know, your tracking cookie itself doesn’t contain identifying information, but it frequently is tied into a backend database, which contains lots of information about how the site has been used.

And I also would argue that, in fact, seems to be a fairly rational tradeoff, where someone can say, here is privacy that I would like, I would like to not be monitored as a user site. If we have that regime, then, of course, we would not expect someone to have strong protections, just as if we had a privacy protecting credit card, where each transaction was completely distinct, and the credit card company did not know -- could not tie those two transactions together. We wouldn't then say please also provide fraud protection.

So I think -- I'm very explicitly saying, if we are an environment where we're going to have the identity carefully monitored by the web service to start with, we should at least derive some benefit from that as consumers.

MR. FELTEN: So if I could say a few words about that, as well. Certainly this point about the -- a tracking cookie being tied to a possibly extensive back end database I think is the issue that -- is the issue of concern for consumers, not as much -- well, the placement of a few bits of -- potentially a little bit of information as the cookie itself on the consumer's computer is not in itself I think the issue of concern, it's -- the issue is the possibility that that will be, in turn, linked to a set of activities that the user has engaged in over time, and that that will get a picture of the user, which may be much more of a privacy issue, concern to the user, than revealing their name to someone. Often what you have done in the privacy of your own computer is the thing that you most want to protect, because it may reveal information that would not be publicly obvious from someone knowing your public identity.

The other issue is, you talked about fraud and fraud detection, in the FTC report, there’s a discussion of fraud detection as being an activity that’s appropriate for companies to do within limits. And it seems to me that the intention is not to prevent a sort of basic fraud detection, but the kind of information gathering and processing and retention that’s needed for fraud detection is different than what is used for other purposes.

And this is an issue we can -- this really gets into the Do Not Track inside baseball, so we might want to take this discussion offline. But the intention is not to prevent all fraud detection.

MR. WEST: There’s a question right there on the aisle.

MS. FORD: Thank you. I’m Sarah Ford. I’m with Bloomberg News. And I was just wondering, what reaction have you gotten from industry so far on the call for Do Not Track, Ed Felten? And what’s your view on the feasibility of an opt-out system versus an opt-in, and, you know, which one are we going forward -- which one do you plan to go forward on?

MR. FELTEN: Well, the reaction from industry, it depends really on which part of the industry, which company you’re talking about. We’ve seen movement by some technology companies toward the use of Do Not Track technologies. Microsoft, for example, announced for the upcoming Internet Explorer 9 a tracking protection technology which is aimed at giving users better protection over tracking. And we may see things from the other browser vendors going forward, as well.

I think a lot of companies have said that they favor the goal of giving users protection against undesired tracking. There is, to be frank, of course, also concern from companies that -- about the impact on the online advertising ecosystem, and we can have a longer conversation about that. I think some of the concerns that we hear in this area are driven by a misinterpretation of what the FTC has been talking about in this area.

Certainly when I read some of the descriptions online about what we are talking about, I don’t recognize our plan in them. But certainly there are some, as well, some legitimate concerns, and these are things that we are actively talking to people about and in which we are eager to get comment. We’re not looking to put entire industry sectors out of business, but we do want to understand how we can protect consumers in a way that still allows innovation to occur.

MR. WEST: There’s another question back there on the other side of the aisle.

MS. EMERICK: Hi, Kelli Emerick with the Secure ID Coalition. I have a quick question and a comment actually on some points that were made. Patrick talked about being reactionary, and it seems like a lot of what we do to try to deal with breaches is reactionary, it's, you know, incumbent upon the consumer to have to monitor their accounts to make sure that there isn't fraud, you know, on their bank or their credit card. It seems like that process is very back end focused as opposed to putting technologies in place on the front end that prevents those transactions from happening in the first place.

I want to move in a little bit different direction and talk a little bit about health care, because there is this movement to move electronic health records online, and as we look at doing that, Ed had mentioned levels of information that needs to be protected, and I would argue that health records are probably pretty high up there in terms of information you want to have protected.

I would argue equal with financial, if not more important. And so how do we look at a market like health care, where at least in the financial sector, there's an incentive to the bank to prevent fraud? Who's responsible for that in the health care sector? And how do we ensure that that information is protected in a way that's really meaningful?

MR. FELTEN: So on the question of health care, it's thornier still because we have, at the moment, an incredibly young and immature market, but as it's shaping up, it looks to be -- the early actors have essentially come forward and said we will provide you with electronic medical record products that are independent of the excellent health system. It would be a separate layer that then the health care industry can interact with, so you will control it.

User control is great from a flexibility, from an individual choice perspective, and there's even been some evidence that it's good for better medical care. The challenge, of course, is all of the security issues that come from taking the responsibility of monitoring. So I agree completely that we need to have a better identity interface particularly when it comes -- and we will see a lot of discussion as the large health care providers learn that actually trying to go through the individual is not the most efficient way of getting health care -- health information, especially if you need to do it quickly or you need to share it when the user is not present. So I think there -- the story is not yet written on that front.

And on a privacy and security perspective, there are some very good voices involved in some of the standard discussions, but there is a very natural tradeoff between that and the providers who said, listen, we're not interested in thinking about privacy and security because health care is more important, and certainly it could really be a matter of life and death. How do we design systems that allow emergency access and that allow for efficient provision of medical care, but still have strong security for the long term perspective and user privacy?

MR. WEST: I mean, I think the big challenge in the health care area is what we're moving towards is greater connectivity, because there are different parts of the health care puzzle that we're trying to connect in order to gain administrative efficiency, figure out comparative effectiveness, what works, what doesn't work. And so I think all the issues that you're highlighting are going to become even more important. And my impression is people actually are more worried about health records being compromised than financial records. I would be more worried about health information getting out than financial information.

Right here is a question.

MR. CROWLEY: Actually, can I just add a follow-up point there?

MR. WEST: Sure.

MR. CROWLEY: I think that it's an excellent issue you raised because the thorniest aspect of that problem, from my perspective, is the data sharing problem. It's not simply a matter of taking stacks of papers that used to just be papers and turning them into digital information that cyber crooks can steal, you know, that's -- the financial services industry knows how to spend money and devise processes to keep digital information safe at a given level of cost, and people are following the processes that they have established. So you can sort of keep information safe at any given cost level, right. Now, how you make the decisions and assign the processes that govern data sharing, who has access to this information, for what extent of time, can they keep copies on their own, that's an exceedingly thorny issues, and I believe that it's in the health care arena where that will play out far more substantively than in any other.

MR. WEST: Okay.

MS. FERNEZIAN: Anna Fernezian with CIT's Identity and Privacy Assurance Group. In this vein of health care and financial, is there -- whose responsibility and how will the FTC and/or the White House National Program Office in the Commerce Department promote customer awareness or consumer awareness of levels of assurance of identity?

Patrick had mentioned about which data is required to have higher levels of identity authentication versus others. I think that we have a problem in promotion of passwords and making them strong, but not necessarily -- and applying it to everything. And, therefore, I think the consumer needs to know that certain credentials need to be stronger for certain levels of information. And to encourage that to the service providers to promote that, so that there is more protection for the consumer, there's more knowledge on the consumer's part, and whose responsibility and how will that campaign get initiated?

MR. FELTEN: As to who’s responsible for consumer education issues, this is something that the FTC has viewed as part of its mission for some time. And the FTC has produced a bunch of consumer education materials about safe online behavior, safe online behavior for kids and so on, and that’s certainly something that is going to continue and expand.

Our friends in the Commerce Department also say that they want to engage in consumer education in this area, and as far as I’m concerned, the more, the better. I don’t think consumers need to be taught to view these issues as important, the real question is, what can they do in a practical way to protect themselves better. And doing that education well is difficult, but I do agree that it’s important for us to do it and do it well.

MR. FRIEDMAN: So I think one of the key things to remember, and the more one spends thinking about privacy and security, the harder it is to remember this, which is that these are very ancillary issues compared to the focus of anyone using any system, which is to use it. And if we are in an instance where there is active consumer choice, you have a multi dimensional problem. Consumers are going to be looking at a number of different features, usability, cost, and, of course, how well, in the case of medical records, how does this impact their medical care.

And in the cases of all of those, privacy and security may not be as important. And certainly having levels of minimum care that are expected either, again, through voluntary self-policing in the marketplace or absent that, some sort of outside regulation I think is very important to have in the space.

It doesn’t make sense just to have competition on a bunch of other dimensions and still have wide variation in privacy and security because no one is going to be thinking about those issues, or a relative few people are going to be thinking about those issues if there really is active competition on other dimensions such as cost or such as quality of service.

MR. WEST: Up here there’s a question.

MR. MORLEY: I’m William Morley. I’m independent, but I use the Internet a lot. In comparing television advertising with Internet advertising, which is connected to cookies, with the television, you get free television because you agree to watch the commercials or look away, whatever, and with the Internet, it’s a little bit similar in that doesn’t the advertising aspect of it, including the cookies and the level of identification of people that are coming to this site, people that are looking at this ad.

Doesn’t that kind of make the Internet free in the same way that television programming is free?

And if you do give everybody the opportunity to turn off all the cookies, that would be like turning off all the ads on television, there wouldn’t be any more programs. And so I’m saying, will the Internet -- will we have to then pay if -- will somebody have to take up the slack of the non-consumers of advertising? I’m interested in the future.

MR. FELTEN: Sure, well, first, to be clear, what the FTC is discussing is not an ability to turn off all ads, nor an ability to turn off all cookies necessarily, although you, in fact, have the power to turn off all cookies in your browser right now, that’s something that you could easily do.

Instead, the goal is -- instead, the idea is to give consumers the ability to opt out of tracking if the consumer chooses to do so. Now, you might choose not to opt out because you -- because you see a benefit to being tracked or to being tracked by certain parties in certain settings. It’s a consumer choice mechanism which is about the tracking rather than about -- necessarily about the showing of ads.

Now, there is this issue that we talked about before, about what the impact is on the advertising ecosystem, and that’s a complicated question. It’s I think pretty clearly not the case that you won’t see ads anymore. You're likely I think to see ads on otherwise free sites going forward. And there's a whole issue to be -- there's a whole complex issue of what the implications of this are and are not for the advertising space.

But first, just to be clear, it's not an opt out, it's not a ban on advertising or cookies, it's consumer choice with respect to tracking.

MR. WEST: Patrick.

MR. CROWLEY: Yeah, that's right. I was just going to add that I think there's no consumer protections issue when it comes to ad supported services. Most everybody gets that. You're watching -- you get the service for free because you're seeing the ad. The consumer protection issue has to do with the implications of what can be known about you. So seeing an ad is an explicit thing. I know that I'm seeing an ad because it's right there in front of me, it's what I can't see that I'd like to be -- that I'd like to learn about, the implications of my habits being tracked over time.

And so, for me, a lot of this boils down to making it explicit to consumers what's being learned and tracked about them so that they can make an informed decision to participate or not, and that's where the danger looks.

MR. WEST: Other questions? Right there.

MR. CERASALE: Jerry Cerasale with Direct Marketing

Association. One of the things, going back to the ads, that clearly Do Not Track does not eliminate ads, it eliminates the ability to try and get more relevant ads, so it decreases the efficacy of the advertising that's left, and therefore, decreases the price that can be charged for giving that advertising, and that's a discussion we can have later.

But going the next step, we do not track, and the fact that if you decide not to allow tracking, if I as a consumer say I don't want to be tracked, and therefore, the Internet site is going to get less money from the advertisers when I'm there, is there a problem with Internet sites charging individuals who opt out of tracking and not charging individuals who allow tracking?

MR. FELTEN: Well, this is a -- let me just say first that, in addressing your question, and I should have said this actually at the beginning of this discussion, that I'm not a spokesman for the FTC. And the FTC, as a body, only speaks by vote of the commissioners, and last I checked, I'm not a commissioner.

So in light of that, let me just say I don't think you should assume that companies will be prohibited from charging or treating differently users who have opted out of tracking.

Certainly one outcome that could occur is one in which companies are free to do that, and do do it, and that in that scenario that would factor into the user’s decision as to whether to be tracked or not.

I think personally that many users not only have no objection, but, in some cases, prefer seeing ads that are more relevant. And so for those users, I think the concern is not about the ads themselves, but about the gathering of information and the possibility of other uses of that information that the users don’t like. And so how to navigate this is an issue which we can discuss at more length offline.

MR. CERASALE: I’m sure we will.

MR. FELTEN: And I’m sure we will. I’m sure we’ll hear from you, and we welcome it.

MR. WEST: Other questions? In the back.

SPEAKER: I just want to do a quick follow-up on the comment about privacy and security in health records, and Allan’s statement about, you know, not necessarily a desire there because you want to get access to it quickly. Can you expound upon that comment a little bit further? And then also I guess is there a distinction in your mind between personal health records, which are something, you know, the industry is putting out for consumers, versus electronic medical records, which is what, you know, we’re talking about in terms of the government funding, to move those forward and get that information happening.

MR. FELTEN: Sure, I think, you know, this discussion could fill many, many different sessions, and there are certainly experts far better than I equipped to talk about it, but I think you hit on a couple key distinctions: the difference between personal medical records, which is what we've seen by some of the early adopter's Microsoft, and Google, among others, and then traditionally controlled -- traditionally institutionally controlled electronic medical records. So we can imagine a world in which hospitals and medical providers only use institutional controlled loans. And the personal medical record, it's nice, it's useful, but it's not actively integrated into the health care provision process, in which case you have a different set of threats because you don't have this interface.

The danger comes in actually having health care providers use these personally controlled medical records either as a way of sharing information between institutions, because you have very strong stovepipes between different hospitals so they're unable to share records directly, so you, you know, route the records through a PMR; or they're actively a way of tracking patient history and learning more about the patient behavior, in which case now you have this information sharing problem that Patrick talked about of who is going to use what, when. And clearly the more useful this record is and the more tightly integrated it is into health care provision, the greater the challenge is in making sure that you have access when desirable, but you don't have access when not desirable.

And there’s been a lot of work done in terms of thinking about this.

One of the challenges is, we don’t really know what good access looks like. We talked about intrusion detection systems earlier at an organizational network level, and one of the things that breaks intrusion detection systems is when users don’t behave in a fairly predictable pattern, it’s then hard to have a white list of acceptable behavior and a red flag list of what is it that we’re worried about.

And I haven’t seen too much research in terms of how patients use electronic medical records through the system to be able to track what is an authorized access and what isn’t authorized.

MR. WEST: Okay, I think we have time just for one last question. We’ll take this question here.

MR. DELBIANCO: Steve DelBianco with NetChoice. Patrick, you expressed a little personal discomfort at not knowing why a targeted ad might be displayed to you. And you might be aware that industry has come up with a recent initiative where you can click on ads that are labeled with a small icon and it will show why is this computer seeing this ad. It doesn’t necessarily say why is Patrick seeing the ad, we don’t really know if you’re Patrick. But industry would then say, well, based on tracking of this computer, we think the person in this computer likes cars and politics and that’s why you saw this car ad. And people are reacting in a relatively benign way to that. They might say, well, I really don't like politics and they'll turn that off, but they're not opting out of tracking because, as Ed said, people are not wigged out about having ads that are more relevant rather than less.

So the question for you, does that satisfy your need to know, to just know what categories drove the ad, or do you feel some need to know how did the advertiser ever figure out I liked cars? Are you interested in drilling down all that click stream history and correcting or revising it, or is it good enough to know what categories are driving your ad?

MR. CROWLEY: That's a great aberration. It's not even so much the display of ads that I think is the thorny issue, so if an organization or a trade group or a company is willing to say here's our best guess at why we showed you this, that's a perfectly valid disclosure to me. What we see time and time again are things that website operators figure out. These are sort of side channels, things they can observe about the browsing behavior that may not be explicitly used to choose which ad to display, but is an additional channel to figure something else out about the identity of the person visiting the website.

Now, this may be an issue that really only matters to unscrupulous types of websites, right, not people who are doing this seriously in business. But I think the key distinction and the broad consumer protection issue is a disclosure of what’s being observed and what’s being done with, well, what user visible options are being taken with that information. That’s the shock that you want to avoid with consumers, oh, I didn’t know that the service provider could do that.

You may notice that mobile operators and credit card firms, they don’t exploit the full extent of what they understand about us, and for very good reason. They have an enormous public perception problem. They don’t want to remind people that they know where we are all the time and they know what we’re going to buy before we buy it, for precisely this reason, because none of us feel particularly comfortable with that.

MR. WEST: But what about five years from now, that may be different?

MR. CROWLEY: It may well be different.

MR. WEST: Allan, were you going to jump in?

MR. FRIEDMAN: Well, I think the really hot button issue, of course, is price discrimination, and there the challenge is very much the I fear getting a very different experience. Now, the other challenges, if you can frame price -- if I designed an experiment, I’d only frame price discrimination positively, I would only get a discount, then I think people would -- you can show people have done for more empirical classic price discrimination, that people don’t have a problem with it.

They push back very strongly when they can envision being on the wrong side of it. If you limit their ability to visualize being on the right side of it, they don’t disapprove.

But I think it comes down to context. So I am okay with -- given the relationship I have with my credit card company, I’m okay with them using their information for fraud detection. However, they can also use information about my purchases to -- you can correlate purchase information with credit worthiness. This now breaks a context wall, that my credit worthiness should be a function of other things, this is a different context. And similarly, I think the uneasiness of tracking is not, as we point out, getting ads that say I’m interested in cars, it’s the uneasiness with a breaking of context, that that information was gained when I wasn’t thinking about cars, and I think that’s the source of the unease.

And if the industry can somehow address that and build that into their models of recognizing that people feel strongly, that behavior in one context should not reflect on other contexts without it being explicitly visible, I think they won’t have nearly as much to worry about in terms of bad publicity.

MR. WEST: Okay. We’re out of time, but I want to thank Patrick Crowley, Ed Felten, and Allan Friedman, and thank all of you for coming out, as well.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

/s/Carleton J. Anderson, III

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2012