

FEDERAL TRADE COMMISSION

I N D E X

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

SPEAKERS:	PAGE:
Russell Schrader	5, 68, 99
Mike Baum	11, 76, 95, 98, 102
Carl Ellison	32, 72, 88, 102
Jim Wayman	47
Margo Saunders	64, 69, 73, 88, 92, 105
Mark Bohannon	80, 91, 101

FEDERAL TRADE COMMISSION

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

In the Matter of:)
GLOBAL-E MARKETPLACE) Commission File No.
) P994312
-----)

Tuesday, June 8, 1999
600 Pennsylvania Avenue
Suite 332
Washington, D.C. 20580-0000

The above-entitled matter came on for
discussion pursuant to notice, at 2:15 p.m.

APPEARANCES:

ON BEHALF OF THE FEDERAL TRADE COMMISSION:

DAVID MEDINE
and
JONATHAN SMOLLEN
and
HANNAH STIRES
and
ROBERT PITOFSKY, CHAIRMAN
and
SHEILA ANTHONY

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

and
MOZELLE THOMPSON, COMMISSIONER
Federal Trade Commission
6th Street and Pennsylvania Avenue, N.W.
Washington, D.C. 20580-0000
(202) 326-3505

For the Record
Waldorf, Maryland
(301) 870-8025

P R O C E E D I N G S

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

MR. MEDINE: Good afternoon. I'm David Medine of the Federal Trade Commission, and John Smollen and our panel here. And obviously we have a good core of people who truly understand the importance of authentication. And obviously you guys are way ahead of the curve with everybody else, so we appreciate your being here. And we do hope to have a good and lively discussion about how communication is important to consumers.

We're going to break this session up into three parts. The first of three demonstrations is how authentication works so we can get a good working knowledge of a variety of authentication tools.

The second will be a broad discussion of authentication issues including cost, convenience, liability, and then the last part of the discussion will be how does this all apply and make sense and become necessary in the international context.

So to start off we'll have three presenters today. The first presenter is Russ Schrader from Visa. He's assistant vice president and assistant general counsel and responsible for managing legislative and

1 regulatory issues.

2 MR. SCHRADER: Thank you. Thanks. Since
3 we're just back after lunch, I'll try to set the stage
4 for the discussion here. We spent the morning talking
5 about a lot of the benefits of E-commerce, the
6 operational cost, efficiency to reduce cycle time, the
7 accessibility, the low costs of the network, the global
8 reach of it.

9 We talked about business opportunities in
10 E-commerce. There are a wider range of things that the
11 internet can do. Government filings, procurement,
12 supply, auctions -- the Ebay presentation is
13 particularly thorough -- content, delivery, payment and
14 bill presentation, securities trading -- a lot of
15 E-traders obviously are at the conference today -- but
16 there still remains a single issue. And we'll take it
17 off to the first slide.

18 And the first slide comes down to at the end
19 of the day, how do you know? How do you know who was
20 sending and who was receiving? How do you know that
21 what was sent is the same thing that was received?

22 The main problem that we identified this
23 morning and is an ongoing theme is a problem of trust.
24 When you're working with open networks, and you're
25 dealing with trust requirements, you need privacy,

1 identity authentication, integrity of the networks,
2 nonrepudiation consistent with each application. Maybe
3 it's the payment guarantee. Perhaps there are other
4 risk management tools, such as interoperability,
5 convenience and global acceptance, like perhaps a brand
6 that's widely recognized as a trusted brand for
7 payments.

8 So let's move on to the next slide, and when
9 you try to establish trust in a virtual world there's
10 several different ways you can do this.

11 One is through authentication, encryption,
12 digital certificates or digital signatures. I'll go
13 into a little bit of each one of those. Now, the
14 easiest is encryption or authentication. Are the
15 parties who they say they are?

16 We're familiar with that today in our everyday
17 booting of a computer when someone asks for a user
18 ID or for a password. When you look at basic
19 encryption, it goes back to a little kiddie decoder
20 ring where you may have a symmetrical key, where both
21 parties are using the same key or it may be a much more
22 tricky one. We use asymmetrical keys, public keys and
23 private keys as digital signatures and certificates
24 that help you represent existing relationships and help
25 you understand who it is that you are dealing with.

1 Look at the next slide. When we talk about
2 that, there's the people and then there is the channel:
3 How do you know that the message you've sent is the
4 same as the message being received? Where for
5 authentication it is, how do you know that the people
6 that you are dealing with are the people that they say
7 they are?

8 When you're sending a secure message and
9 receiving a secure message through a type of channel
10 encryption like SSL, which we talked a little bit
11 about, you see that there are good security in the
12 channel but there are existing risks. And those are:
13 no identification, no digital signature, there's no tie
14 to a payment system when you're talking about
15 conducting E-commerce, and there is an open potential
16 for fraud in terms of some of the authentication
17 issues.

18 Let's go to the next slide and you can see the
19 value of authentication. Here you're dealing with a
20 digital signature. The digital signature is not a
21 digitized signature. It's not, you know, John Doe in
22 script reduced to ones and zeros so that is reproduced
23 at the bottom of something. It's basically a string of
24 data that has been encrypted. It's something that can
25 be used through public keys and private keys that ties

1 into a relationship.

2 In the case of Visa and the SET I'll talk
3 about, it's a banking relationship where identification
4 can be endorsed through trusted third parties. It
5 could be banks. It could be Visa. It could be
6 Idenitrust. It could be Verisign. It could be any
7 hierarchy of trusted parties that help establish this
8 identification and who will stand behind that trusted
9 identification. And also, this does leave a little
10 less potential for fraud.

11 Now, when you look at the top of this, you see
12 that we are a dealing with asymmetric keys or public
13 keys. What you will see is that there is a private key
14 that each one has and a public key that is posted on
15 the web. These are two different, but they are
16 mathematically related keys. And each one has
17 available to that that helps you encode a message
18 through what's called a hatch function, but at the
19 same time allows it be received by someone who can
20 access it and decode it.

21 Moving to the next slide, one of these ways of
22 dealing with encryption authentication is something
23 called secure electronic transaction or SET. There are
24 certainly other protocols out there that may provide
25 equal or enhanced specific protection. It depends what

1 you are trying to do. You can have a client based
2 digital signature that you could use with SSL. You can
3 have other kinds of protocols and other kinds of
4 digital signatures and encryption devices, but what SET
5 was devised for in the payment system, in the joint
6 payment system was to create an open specification for
7 secured payment cards over an open network. And it was
8 designed to reenforce an existing, trusted financial
9 relationship.

10 You will find on the next slide a little bit
11 of an overview of how SET works. You see the security
12 standard that we've talked about. You see how each of
13 the cardholder and the merchant has an ability to
14 create a message that would be encrypted and sent
15 through a secure channel and then taken down by the
16 other parties and then electronic commerce facilitated
17 through an existing Visa system protection.

18 There are, however, if you look at the next
19 slide, and moving on to the next slide, a little bit
20 more of a detail as to how SET works. And you can see
21 we've placed an order over the internet. You would
22 sign it and encrypt with your digital certificate and
23 with your key.

24 It would be picked up by the merchant. This
25 would be a one-click thing. It would be completely

1 transparent to you when you got there and to the
2 receiver, and then you would authorize as an existing
3 Visa purchase order authorization through settlement.

4 There are clearly disadvantages to any of
5 these encryption and authentication issues. There is
6 still secrecy if you're using symmetrical keys and not
7 asymmetrical keys. If you're only using one public
8 code, that code may be stolen, and secrecy there is
9 still a concern.

10 You need to determine that the public key
11 truly belongs to the owner of the public key and that
12 is basically the function of this certification
13 authority, to come up with the authentication of the
14 identity, or the other attributes that are represented
15 by the CA. And when you have your digital certificate
16 that sort of says John Doe, here is your key, here is
17 your ID number, here is what you should have in order
18 to do this, it's only as good as its issuer and the
19 trusted relationship behind that.

20 In SET, that neutral trusted third party for
21 certification is the banks. It's the bank who knows
22 you who has issued your Visa card in my case, and it's
23 the banks who is acquiring or working with the
24 merchant. So I think that's kind of the background of
25 authentication digital signatures as well as a very

1 brief explanation of how SET works.

2 MR. MEDINE: Actually we have four presenters.
3 The next presenter will be Mike Baum, who serves as a
4 vice president of practices and external affairs for
5 VeriSign where he oversees the company digital ID and
6 VeriSign Trust Network Operations.

7 MR. BAUM: Thank you. If you would permit me
8 to wait until my slides get going, I'll pick up at the
9 same time.

10 MR. MEDINE: Just while that's going on, let
11 me say as a ground rule this morning's ground rule was
12 that we are not going to focus on privacy issues. This
13 afternoon's ground rule is we are not going to focus on
14 the encryption debate. We'll leave that to other
15 agencies and other forums. We will assume that there's
16 adequate encryption to conduct consumer transactions
17 and precede on that basis.

18 Mike.

19 MR. BAUM: Sure. Now, we'll get started.
20 First of all I'm delighted to be here from Verisign and
21 obviously these are important issues. There are vexing
22 questions. Nobody has all the answers, to say the
23 least, and so to speak, we're all in this together to
24 make the environment better hopefully as quickly as we
25 can.

1 One other initial comment is my time is quite
2 limited today, so I had to decide whether to leave some
3 slides in that I wouldn't necessarily have time to
4 fully address to the extent that they will at least
5 appear on the ultimate FTC web site if they'll have
6 them. So I'll just race over a few slides, and we can
7 always come back to them at a later time.

8 Next slide, please.

9 What is Verisign? I suppose other than
10 talking about a Visa, everyone knows who they are,
11 Verisign is this crazy thing called a certification
12 authority that issues digital certificates and manages
13 certificates. And it, in fact, goes well beyond that
14 in terms of what we're doing today.

15 Next slide, please.

16 What we are effectively doing is establishing
17 a global infrastructure of affiliates that
18 correspondingly manage certificates within the scope of
19 their geographic area or their service area. So
20 effectively we are managing on a global basis a cogent
21 set of policies to provide for interoperability on a
22 global basis, and this is for a broad range of
23 applications, some of which I'll be describing in just
24 a few minutes.

25 Next slide, please.

1 What I don't have time to do is to get into a
2 PKI 101 course right now, so I'm going to gloss over
3 the next couple of slides, but suffice it to say that
4 of course underlying the technology here is the use of
5 asymmetric cryptology, which provides use of dual keys
6 and can be used both for authentication and integrity
7 purposes as well as for ultimately assuring
8 confidentiality of information, all of which, of
9 course, is a function of how it's implemented with
10 respect to particular applications. Beyond that, I'm
11 not going to jump into that slide.

12 MR. MEDINE: Mike, maybe if you could just
13 maybe give the beginner's view just so people
14 understand briefly how the public key, private key
15 interact in terms of --

16 MR. BAUM: Certainly. There is at least one
17 noted scientist on this panel. So if I get it wrong,
18 correct me. But again, just at the highest level what
19 distinguishes this technology in part is the fact that
20 each person, rather than just having one key or sharing
21 it as you heard before actually has a cryptographic key
22 pair. This is basically just a bunch of numbers, if
23 you will, using certain mathematical algorithms or
24 cryptographic algorithms that will produce this key
25 pair. It's composed of two.

1 Effectively what it is is a public and a
2 private key. The private key, which is one of the two
3 components, is generally understood to be private by
4 you or by your organization. It's a function of how
5 it's implemented. It's secret. You never tell anybody
6 that key. What you do is you use that key to create
7 what are called digital signatures or alternatively to
8 decrypt messages, again depending on the algorithm that
9 is used.

10 For example, if I wanted to digitally sign a
11 document to Mark Bohannon, who is sitting on my far
12 right, I would on my computer -- hopefully it would be
13 fully transparent, but I would create a message and
14 could basically click to sign it, enter in a pass word,
15 whatever else, that would gain access to the private
16 key that sits on my computer or on some type of a
17 hardware device, such as a Smart Card. It would bait
18 the computer, then, using that private key and using
19 information from the message itself would create a
20 transformation called a digital signature.

21 The digital signature, again, is just a number
22 that's unique to the message and largely unique to the
23 key that I used to create it.

24 So on every message that you create you would
25 have to theoretically have a different digital

1 signature. So over your lifetime you may have, again,
2 theoretically, an infinite number of digital
3 signatures. It's very different than a PIN or a pass
4 phrase that is not typically dynamic. If this were
5 disclosed over the net, of course, it would be a great
6 security violation.

7 So some of the interesting characteristics
8 of this technology are such that when I create a
9 digital signature and append it, say to a contract or
10 other message that I send to you, that anyone,
11 including an interloper or a bad guy, if you will,
12 could grab that digitally signed document and having
13 that digital signature attached to the message. It
14 would not do them any good. They would not be able to
15 modify the message, such that the recipient upon proper
16 verification of that message would not be able to
17 determine that the message had been modified since the
18 time that the digital signature was created.

19 MR. MEDINE: And the converse of that is that
20 the recipient of the message can know with a high
21 degree of certainty that one and only one person could
22 have created that and that is the one person that has
23 that private key?

24 MR. BAUM: Right.

25 MR. ELLISON: What it knows is that one and

1 only one private key created it.

2 MR. BAUM: And Carl will tell you later that
3 of course one of the issues is, in fact, a critical for
4 requirement for the use of this technology is that the
5 private key of the originator remains secret to him or
6 whoever the owner or appropriate user of that code
7 might be. If that key is disclosed, of course, then
8 you can't trust the message. It's pretty obvious.

9 We'll move right along to the next slide,
10 which I will not get into for want of time. But
11 basically there are two boxes there. The one on the
12 left shows that basic function of a message in the key
13 being the two key critical pieces of information that
14 create the digital signature and then on the receiving
15 side basically going through the process of
16 verification. The bottom line is if the recipient has
17 a true copy of the public key. Remember I told you you
18 had a key pair, a public and private key pair that have
19 a unique mathematical relationship to them.

20 So the public key, if it's properly
21 distributed, and that's a whole other discussion we'll
22 be getting into, but provided the recipient has my
23 corresponding public key or more importantly Mark
24 Bohannon has my corresponding public key, then he can
25 verify that message that I sent to him and

1 determine that it did, in fact, come from me provided
2 that my key had, again, been properly secured.

3 MR. MEDINE: Just also to clarify, it sounds
4 like it's serving two purposes. One is to verify the
5 identity of the person who inputs or is using the
6 private key but also to assure that that message in its
7 entirety is the message that that person sent
8 unaltered.

9 MR. BAUM: It provides integrity assurance of
10 the message. If you changed one single character in
11 that contract, the digital signature would not verify
12 by Mark, and therefore, he would know that there had
13 been something wrong with that communication, and then
14 he should therefore probably not trust the message.

15 And, again, depending on the algorithm used,
16 you can also use this analogy not just for authentication
17 purposes, but also to secure the confidentiality of
18 communications, such that if I wanted to send Mark a
19 secure message that only he would be able to read,
20 provided -- and if I knew his public key, I could
21 encrypt the message in his public key and that would
22 only be able to be decrypted with the corresponding key
23 which to the extent that Mark was the only person that
24 had his private key, he would then be the only person
25 that could decrypt it.

1 So it's a very powerful technology and one of
2 the messages you'll see that I raised later is that
3 when you think about the possible relation of this
4 area, and we must also recognize that the use of this
5 technology and certification infrastructure for
6 confidentiality purposes is very real and very powerful
7 and simply may have a different set of requirements
8 from the regulatory perspective.

9 Next slide, please.

10 So I said before that if I were to send Mark
11 Bohannon a message, then it was critical that he, in
12 fact, had -- he knew what my public key was so
13 that he could properly verify it. How is it that he
14 would know what my public key was? Well, of course, I
15 could have met him in a bar somewhere and if he knew me
16 personally, I could hand him my public key and then
17 he'd have confidence that it had indeed come from me.
18 But realistically, and again thinking through what type
19 of commercial infrastructure is being considered or
20 employed, one more efficient method of doing that is
21 through the use of what are called digital
22 certificates.

23 A certificate is no more than a digitally
24 signed data file that contains certain information and
25 perhaps at a minimum it would contain my public key.

1 It may or may not be associated with my name or some
2 other attributes, but at least it would contain my
3 public key and would be signed by a certification
4 authority or some entity that you trust.

5 So if Mark had my certificate to the extent
6 that he could verify the digital signature on the
7 certificate, it would be a digital signature of some
8 trusted third party, maybe even the U.S. government or
9 Verisign or some other entity, then he could trust the
10 information contained in that certificate, that is, he
11 would be able to trust that my public key had some
12 association with me. And if that were the case, he
13 could now use my public key to verify the message when
14 he receives it.

15 Does that sound complicated? Well, maybe, but
16 effectively one of the things that is very important
17 and is happening is that this technology is being made
18 more user-friendly and more transparent, so that a lot
19 of it goes on behind the scenes. And, of course, the
20 fact that it goes on behind the scenes could be another
21 issue that could be raised in terms of its capability
22 of being appreciated and assessed.

23 Nonetheless, this really can become
24 increasingly very transparent. As a matter of fact, set
25 up protocols that are simply overlaid over existing

1 messaging and related systems. Next slide.

2 So what are the use of these digital
3 certificates and the use of digital signatures and this
4 technology? Well, you've heard Visa talk about the use
5 of the technology in terms of the payments and, of
6 course one of the protocols -- well, it's taken off
7 more in Europe than it has here, but it's this protocol
8 called SET that he mentioned represented in the lower
9 left-hand corner.

10 Another protocol that you've heard from the
11 professor from Utah, I believe, earlier today, he
12 mentioned, well, if the little lock closes on the
13 computer, the little key comes together on your
14 browser, and that typically is an indication that the
15 SSL protocol, secure socket layers, it was mentioned
16 earlier has been used. So that would be provided for an
17 end-user being able to authenticate a browser or who
18 was operating the browser. And there are many other
19 applications, including just simply secure E-mail,
20 virtual private networks and a host of other
21 applications that just continue to crop up.

22 Next slide, please.

23 One of the key points that I want to make
24 today is that when you think about a certification
25 authority, do not think about it in a monolithic

1 fashion. One size doesn't fit all. If you're going to
2 think about regulating certification authorities,
3 remember that Microsoft is even putting out a product
4 right now that allows anybody to become a certification
5 authority. So grandma could be a certification
6 authority for her knitting club. So how will you
7 ultimately regulate or put out regulations in terms of
8 trustworthiness or other related requirements when it's
9 being used for even communities of interest, if you
10 will, that may be as mundane and as voluntary and as
11 nonprofit, if you will, as a knitting club?

12 I won't run through the other options, but
13 just as long as you understand that the nature of
14 certification and the types of certification
15 authorities that will be out there will range from
16 government to private sector to informal to more formal
17 to whatever, and it's really a blooming of a thousand
18 flowers out there.

19 Next slide, please.

20 The other point to make is when we think about
21 certification authorities, again, from another
22 perspective, don't think of them as
23 monolithic authorities. That is, it's not just a
24 single entity that is evaluating someone's credentials
25 or other information to make a decision as to whether

1 or not to issue the certificate to that person or
2 entity. Instead, one of the things that we can observe
3 in the industry is at a minimum a bifurcation between
4 the back end of the certification infrastructure and
5 front end up, such that the front end might be what is
6 often called a registration authority.

7 You can think of a registration authority as
8 just the entity that decides whether or not somebody
9 should be approved for issuance of a certificate. It
10 could be the Department of Motor Vehicles that makes
11 that decision, but once it makes the decision, it sends
12 the actual certificate issued over to an IS -- an
13 information systems resource within the government.

14 From the private sector, it might be a company
15 such as Verisign offering given corporations the
16 ability to set up a registration authority using a
17 browser on their site to make the decision as to
18 whether or not to issue certificates to employees, but
19 then sending cryptographically secured approval
20 messages to Verisign who actually issues certificates.

21 So we need to distinguish between the entity
22 that issues the certificates physically, and the entity
23 that actually undertakes the registration.

24 Next slide, please.

25 And going beyond just a notion of

1 certification authorities is this notion of a PKI or a
2 public key infrastructure, and there's a definition of
3 it up there. From the internet space you can think of
4 it simply sitting on top of or using the internet and
5 ultimately supporting many different possible
6 applications.

7 Next slide.

8 And when you think about the notion of a PKI,
9 or for that matter even a certification authority, it
10 is a lot more than just a piece of software. And those
11 are at least a few of the attributes that perhaps a
12 modestly trustworthy certification authority or series
13 of certification authorities within a PKI might, in
14 fact, want to have in place.

15 So, of course one of the tough issues both for
16 government and the private sector is ultimately how do
17 we assess the trustworthiness of these infrastructures.
18 And at least on the back end those are some of the
19 features we may be concerned with.

20 Next slide, please.

21 Now, a few paradigms over the next couple of
22 slides, again, just for the purpose of perhaps modestly
23 thinking through some of the issues that one might want
24 to think about if indeed regulation was ever
25 contemplated.

1 The first certification authority is not
2 necessarily just a freestanding entity doing something
3 just inherently new, but effectively think about it
4 also as an overlay or enhancement to the existing
5 infrastructure, perhaps one of the better examples
6 would be what Visa mentioned to the extent that they go
7 off and they spin up a SET implementation or secure
8 electronic transaction and people are then sending
9 their credit card information using this
10 technology.

11 There's already a whole slew of regulation out
12 there. Regulation of what, reg E and Z, whatever,
13 would be fully applicable and already in place. So the
14 mere fact that you're now using certificates is not
15 necessarily an indication to think through a whole new
16 regulation scheme just merely because you're using the
17 technology.

18 In fact, the argument in that case would be
19 what you're doing is even simply enhancing the security
20 of preexisting systems. Another issue is that,
21 again, we're not only talking about authentication in
22 terms of what certification authorities do as I
23 mentioned earlier, but also that they can be used for
24 confidentiality. And if they're being used for
25 confidentiality, I think a different set of paradigms

1 might apply.

2 Since applications vary, so might the
3 regulations. We held a consumer workshop or a workshop
4 that considered some consumer issues with PKI recently,
5 and that was perhaps the strongest message in so many
6 words. You have to look at it on an application
7 specific basis. And as Carl may or may not opine on
8 later, there's an issue as to whether or not certificates
9 should ultimately provide for some assertion as to an
10 individual or a company's identity versus their
11 authority, and there's lot to be said for the use of
12 certificates for many other different purposes; and
13 clearly there's tremendous benefit, probably growing
14 benefit, for the use of certificates to make assertions
15 about the authority of someone.

16 For example, are they authorized to practice
17 law? Do they have the right to write checks for their
18 companies or whatever? But the real bottom line is,
19 hey, the certification authorities out there to some
20 extent will issue certificates as a function of market
21 demand. And like it or not, the reality is that the
22 market demands right now are for identity or
23 identity-like certificates as well as authentication
24 certificates. So again, let a thousand flowers bloom.

25 Lastly, not necessarily a message

1 intermediary. When you think about any kind of a
2 regulatory scheme with certification authorization,
3 don't make the assumption that they're involved
4 intimately with every single transaction.
5 Certification authorities under some paradigm could
6 issue certificates and never touch or have anything to
7 do with them unless there's a revocation issue. And
8 I'll get to that a little bit more later.

9 Next slide, please.

10 There's also then continuing on this point, on
11 this nontransactional model, when you think of Visa, or
12 a similar payment mechanism, every time a consumer
13 takes the credit card, it is likely going to be done in
14 this country, it will be an on-line approval or an
15 authorization for use of that card. But it turns out
16 that when you think about CAs, yeah, there are models
17 where that may invariably be the case, but there are
18 other models where they're not involved in the
19 transactions. And what I'd like to urge is there may,
20 for appropriate transactions, be clear consumer
21 benefits. And let me tell you what they might be.

22 First off, enhanced privacy. Gee, now a
23 consumer can use a digital certificate to send an
24 authenticated message or a confidential message
25 and the certification authority will never know.

1 Nobody will have access to that content or message
2 except the end parties.

3 Or, over here, facilitates unlimited use.
4 Once the certificate is issued under some models,
5 unless they are regulated out of business, the consumer
6 can send effectively an infinite number of
7 communications with that certificate, whether to
8 authenticate or to make that information confidential.
9 And they're not going to be hit up with a 2 or 3
10 percent fee for every transaction, okay, or at least a
11 corresponding merchant. So again there is an economic
12 potential benefit.

13 And lastly, I grabbed the last ones there.
14 Again, this notion of unlimited use.

15 Next slide.

16 One more important paradigm, if you will,
17 before I quickly move on to a number of other issues.
18 There's been a tremendous thrash among the pundits as
19 to the propriety of open versus closed systems. And
20 the whole notion here in part while there are many
21 different definitions for open or closed, the notion is
22 that if something is closed, it's, you know, it's a
23 very intimate community and everybody has got a
24 contract signed with all the parties and everyone knows
25 their rights or obligations.

1 Unfortunately, I would claim that the
2 discussion typically on open versus closed turns out to
3 be no more than an eloquent set of fighting words,
4 because effectively what we've seen is that many
5 systems will effectively by way of web rats are
6 ultimately on-line providers for allowing a user to
7 contract and effectively become part of, if you will, a
8 very large or more dynamic closed system.

9 Next slide, please.

10 On the whole area of private key protection,
11 there's not a lot of time to get into it right now,
12 although perhaps this may come up later during the
13 discussion. But the point I'd want to raise is that
14 for so many systems with the tens of millions of
15 browsers that are out there, that consumers are really
16 primarily using, those are not necessarily owned,
17 operated or controlled by certification authorities.

18 They're owned, operated or controlled by the
19 Microsofts, the Netscapes, or the other manufacturers.
20 And the question is where are they at this table? They
21 ultimately control that piece of software, have the
22 greatest amount of control over the interface, the
23 greatest control over whether or not the cryptomodules
24 that hold the private keys are, in fact, protected.
25 And it's very important that we think about those

1 parties in the broader schemes of rights and
2 responsibilities.

3 Why don't I move on to the next slide?

4 Also, by way of Verisign, for example,
5 offering consumers enhanced mechanisms to protect their
6 private keys are important. And here is at least one
7 of our web pages where in fact we are offering Smart
8 Cards to consumers if they want them to enhance the
9 protection of their private keys.

10 Next slide.

11 Also, of course, the notion of trust
12 credentials. How do you know which certification
13 authorities to trust? Well, I hope there will be a
14 discussion at some point of mechanisms for assessment
15 on a very broad global basis. But for want of that,
16 some of the criteria or attributes of trust are some of
17 the things listed there. And I claim that one of the
18 big ones is a very rigorous recognized, detailed audit
19 of the infrastructure, and there are many different --
20 there are an increasing number of programs where they
21 ostensibly provide these types of audits, but it's an
22 audit not only where you have purportedly good
23 procedures, but indeed whether you are following it,
24 which is the second half and the much more costly half;
25 and that means a fair amount of work. Why don't I just

1 keep moving?

2 The last point I wanted to raise where it
3 says future. Browser Root Policies. One of the
4 interesting things going on that one can observe over
5 the last six months to a year is that the major browser
6 manufacturers are now setting criteria for the
7 certification authorities to actually include their
8 public keys, their root keys, in the browsers, and I
9 think you're going to start to see more focus on what
10 those criteria are as a gatekeeper of trustworthiness
11 that, of course, will affect the consumer in its use.

12 Next slide.

13 Offering enhanced insurance has been raised by
14 other speakers at this program today, and, of course,
15 Verisign offers the Netsure Protection Plan, which was
16 the first one, I believe, that was out there offering
17 enhanced warranty protection to users.

18 Next slide.

19 Just to mention, there has been a lot of work
20 in this area, and while not every one of the provisions
21 and paradigms listed in these -- the guidelines that
22 are up there and now the work on the PKI assessment
23 guidelines -- will necessarily be agreeable to
24 everyone. The bottom line is as we begin to think more
25 about the rules and the problems out there, it's at

1 least worth taking note that there is a fair amount of
2 work being done out there in the field right now.

3 Next slide.

4 Again, to wrap up, I did want to notice
5 one interesting initiative right now. While, of
6 course, the use of disclosure technologies and
7 disclosure from a consumer perspective is certainly not
8 adequate, and I've learned that from some of the
9 experts in the field, it certainly is at least an
10 important step; and in that regard one thing I can
11 announce today is there has been a fair amount of
12 progress made in the development of a succinct, brief
13 proposed model disclosure statement for PKI's that can
14 be used either by freestanding PKIs or by even existing
15 companies simply deciding to deploy this type of
16 technology.

17 What you see listed up there are some of the
18 issues that seem to review -- to actually move forward.
19 I'm just about wrapping up now. Next slide, please.

20 Now, just to mention there was with the
21 information security committee of the ABA workshop on
22 consumers and PKI, and there will be another one in the
23 fall. If anybody wants information, see me after the
24 program.

25 Next slide.

1 And also just to note that just last week
2 among representatives of the PKI industry, there is now
3 the go forward and will likely be a press release quite
4 soon establishing finally a PKI industry association.
5 And I know regulators always like associations so that
6 they can get some kind of industry-wide accountability.

7 Next slide, please.

8 I'm just wrapping up with some references, and
9 those are the end of the slides. Again, thank you for
10 your patience.

11 MR. MEDINE: Thank you very much and that was
12 extremely helpful in educating us about some very
13 complex, technical issues.

14 We are very lucky to have our next speaker
15 here, Carl Ellison. You can imagine when the Federal
16 Trade Commission called Intel and asked one of their
17 employees to come to the FTC hearing room, that caused
18 some apprehension back at home. Carl was willing to
19 come nonetheless, and we appreciate it.

20 MR. ELLISON: Thank you.

21 MR. MEDINE: He's a security architect for
22 Intel.

23 MR. ELLISON: Thank you for the opportunity to
24 come here and talk. You're correct. When they told
25 people I was coming here, there was a great deal of

1 apprehension and then I told them why, and they
2 relaxed.

3 I'm here to talk about some security concerns
4 that we have that we need to have when using digital
5 signatures. I'm a cryptographer and as a
6 cryptographer, I very much -- by the way, I very much
7 enjoyed Michael's description of public encrypto. That
8 was right on. It was very good. And, of course, I'm
9 very fond of this technology, but in spite of being
10 fond of this technology, there are some things we need
11 to worry about.

12 One thing we know, and Michael pointed it out,
13 is if you change one character in that digitally signed
14 message, then that signature no longer verifies. This
15 makes a digital signature something much stronger than
16 a handwritten signature. You can do a handwritten
17 signature on a document and have it changed after the
18 fact. The trouble is that a digital signature is not
19 the same as a handwritten signature. A handwritten
20 signature is a biometric, which -- it's not perhaps the
21 best biometric, but it is a biometric. It's produced
22 by the action of human muscles. A digital signature is
23 produced by a machine.

24 So I would like to use the next slide talking
25 about mechanical signatures. Next.

1 The old check-writing machines impressed me as
2 a child. My father had a small company, and that
3 company had a check-writing machine, and I was, I
4 guess, five years old, and I loved to see this thing.
5 And I talked him into letting me stamp a blank piece of
6 paper one day, because it made all these pretty raised
7 bumps in red and blue. And it had all these levers for
8 numbers and this big wooden handle that you pull down
9 to go ca-chunk and write a check with it.

10 What I've learned recently is that these
11 machine signatures are not valid. There's case law
12 apparently -- I'm not a lawyer, but I'm told that there
13 is case law to the effect that these signatures are not
14 valid.

15 Next.

16 But they are allowed if you have a specific
17 contract between the owner of the machine and the banks
18 that is alleged -- supposed to receive these signed
19 checks. The reason that you -- next, please.

20 The reason it's not valid is you don't know
21 who pulled that handle. In fact, in my father's
22 office, I pulled the handle as a five-year-old.

23 Next.

24 You can't -- there's nothing that presented in
25 this -- in this raised set of bumps in red and blue

1 with an embossed number, there's nothing in that
2 tells you anything about who pulled the handle.
3 So there's nothing you can take to court to show
4 who pulled the handle.

5 Next.

6 But if you have a contract between the owner
7 of the machine and the bank, you don't need to prove
8 who pulled the handle. The contract will say that the
9 bank honors this and the owner of the machine will not
10 dispute it.

11 Next, please.

12 The problem we have today is the digital
13 signatures are less secure than the mechanical
14 signatures of that check-writing machine, less secure
15 in spite of the fact that they have these wonderful
16 property that if you change one character, the
17 signature is no longer valid.

18 The first reason they are less secure is you
19 do not know who pulled the handle. In this case
20 pulling the handle is pressing enter on your computer.
21 You don't know who pushed that key, and you have no
22 evidence about who pushed that key that you can take to
23 court.

24 Next slide.

25 Another problem we have with public key

1 technology on a digital computer is that my father put
2 his check-writing machine into a locked safe, and he
3 would take it out -- once he took it out to let me play
4 with it -- but he took it out only when he was going
5 to write checks, and otherwise it stayed in that safe.
6 But a digital computer is too expensive and has too
7 many uses to be put in a safe except when you're going
8 to take it out to write checks. The exception to this
9 might be the computer that Verisign uses for their high
10 value keys. I've been to Verisign. I've seen the safe
11 that they keep it in.

12 So in that case -- in some cases you do put
13 the computer in a safe and you do protect your keys
14 that way, but in general you will not be putting the
15 computer in a safe.

16 Next bullet.

17 And what's worse is the real handle that you
18 pull is not this big wooden handle that I had a tough
19 time with as a five-year-old. It is, in fact, not
20 advisable to the user. It is just software, and it can
21 be fooled by a virus. You know, Melissa 12, whatever
22 the virus is that will come out and will go around
23 signing things, with private keys that it discovers.
24 And that kind of attack, the virus attack, is not
25 noticed by the person who owns the private key, so you

1 can't even report that something went wrong. It's not
2 as if his credit card or smart card was stolen. The
3 smart card was still there plugged into the machine.
4 At night he takes it out of the machine, puts it in
5 this pocket and goes home. But Melissa 12 signs
6 something with that smart card without his knowledge.

7 Next slide, please.

8 Now, I claim that businesses can still use
9 digital signatures and use them well because -- and
10 we'll go through a set of bullets.

11 Next bullet.

12 Specifically, you can do business to business
13 EDI based on a contract between the two firms doing the
14 business, the same kind of contract that made a
15 mechanical signature valid can make this digital
16 signature valid between these two firms.

17 The next is -- we can just do the rest of the
18 bullets. The business can put its digitally signing
19 machines under surveillance and can watch their use.
20 It can put locks on machine rooms and locks on the
21 purchasing department office.

22 It can use secure work flow for high value
23 signatures. Secure work flow is a process that we are
24 working on in Intel and a number of others, I'm sure,
25 in which you have multiple parties that have to be

1 involved before a signature will be made. And each of
2 those parties authenticates itself to authorize this
3 final signature.

4 You can have single-use machines in a
5 business. You wouldn't have that at home. I mean, it
6 might be nice if everybody went out and bought a
7 separate computer for every function. That would be a
8 lot of Intel chips. That would be nice, but that's not
9 going to happen; but it might happen in a business.

10 Furthermore, businesses have fire walls and
11 other network security, hopefully to prevent Melissa
12 12 from coming in and doing digital signatures, and the
13 final bullet. Businesses often, at least Intel does,
14 as I'm sure that most businesses do, have a policy
15 against loading strange code on your machine, code that
16 might introduce viruses.

17 Can we go to the next slide?

18 There is a place, I believe, for home user
19 signatures. The first would be low risk applications.
20 For example, I have -- my bank offers me a web page
21 that let's me move money between my checking and my
22 savings account, I would be very happy to authenticate
23 that by digital signature. Right now all they let me
24 do is passwords. I'd much rather have digital
25 signatures for that, but that's a low risk application.

1 The most that can happen is the inconvenience of having
2 my money in the wrong account. No one can move money
3 out of my account into their account with this
4 mechanism. Or I can do purchases under the credit card
5 mail order telephone order rules, because those are
6 relatively low risk. Under those rules, I can dispute
7 line items on my credit card statements, and I am
8 assumed correct until the merchant provides hard
9 evidence to the effect that the transaction really did
10 occur.

11 And, of course, we can always use signatures
12 on home machines for known value applications, signing
13 E-mail or authenticating access to personal web pages.
14 These are applications of so little value that they
15 would not be attacked anyway, but I would be very
16 nervous about using a home computer for any high value
17 digital signature, because we will not see the
18 protections on the home computer that a business might
19 be able to put into place. We will not see single-use
20 machines. We will not see machines in access-
21 controlled rooms. We will not see machines under
22 video surveillance. We won't have fire walls. We
23 will not have provisions against downloading strange
24 code. If you have a teenager in the house, you
25 know first thing there's going to be a lot

1 of strange code downloaded on this home computer.

2 So we go to the next slide.

3 Now, I've got two more slides, and these are a
4 short quiz on computer security that I wrote. I will
5 ask for a raise of hands, a show of hands for this
6 quiz.

7 The first slide, and this ties directly to one
8 of Michael's slides, and thank you, Michael, for
9 introducing this. I have in this model two different
10 computers. The left column is a desktop computer. It
11 might be at a business. It might be a home computer.
12 You know grandma's knitting club computer or it might
13 be some, you know, IT computer at work, but it's a
14 normal desktop computer, and it's not specially
15 protected. It's not in a locked room. It's not under
16 video surveillance, so it's reasonably attackable.
17 But on the right we have the ultimately protected
18 computer. This is in a locked room with video
19 surveillance, with strong personnel procedures,
20 probably multi-party access control so you have to have
21 two or three persons anytime you get near this
22 computer. So I've got three cases for issuing
23 certificates.

24 Case A, the certificate is issued just by a
25 certification authority in that Fort Knox.

1 Case B, it's issued by the CA in Fort Knox,
2 but on direction from a registration authority held on
3 the desktop.

4 And case C, it's issued by a CA in that desk
5 top machine.

6 And in black print I show where the client is,
7 the client for whom the certificate is being issued.

8 In case A, the client is on the phone or the
9 net talking into Fort Knox.

10 The in case B and C the client is at the desk,
11 at the desktop machine.

12 Now, the question is which is the most secure?

13 I'd like a show of hands who thinks A is the
14 most secure. Nobody. Okay.

15 MR. MEDINE: One.

16 MR. ELLISON: One? One thinks A is the most
17 secure.

18 Who thinks B is the most secure? Four? Four.

19 So one, four, and who thinks C is the most
20 secure? One, two -- seven people in the room.

21 MR. MEDINE: A lot of abstention. There
22 should be a fourth opportunity to say it depends.

23 MR. ELLISON: It depends.

24 MR. MEDINE: Or I don't know.

25 MR. ELLISON: Actually, I claim it does not

1 depend. My answer is that C is more secure than B, and
2 B is more secure than A; and I put this slide up on
3 purpose because this is counterintuitive.

4 The reason that A is less secure than either B
5 or C is not a security problem with Fort Knox. That CA
6 is solid. The key that's used in that CA is well
7 protected, will never be revealed. The problem is this
8 client is on the phone or over the net, and it is very
9 easy with no security or crypto expertise at all to
10 engage in identity theft over this phone connection.
11 Run of the mill criminals know how to do that today,
12 and so the easiest attack anywhere in that system is
13 the attack on A.

14 Now, B and C don't have that attack. My
15 assumption there is the operator of the desktop
16 machine knows this client. You know, it might be my
17 bank for example. He knows me, my branch bank who
18 knows me or it might be my IT department at work who
19 knows me, so that attack is not open. That makes B and
20 C more secure than A, but C is more secure than B by a
21 small amount because it makes fewer components.

22 Every time you add a component to a system,
23 you decrease its security, with some small exceptions,
24 but none that show up in this diagram.

25 So next slide, please. And once more.

1 The first question for electronic commerce, it's
2 been said occasionally, although I haven't heard it yet
3 today, that electronic commerce needs the deployment of
4 a PKI in order for it really to succeed. How many think
5 this is true? One.

6 How many think this is false? Seven. Okay.
7 That's good, because I agree with you there, and the
8 evidence for that is there is no real PKI yet and
9 electronic commerce is succeeding just fine.

10 Next section.

11 And the next one is -- this is the last one,
12 last part of this quiz -- we know -- and before going
13 to Intel I was at Cybercash as a cryptographer for
14 Cybercash where I dealt with this specifically -- we
15 know the computers need security in order to do -- in
16 order for electronic commerce to succeed. We keep
17 hearing this from consumers. We hear it from surveys.
18 We know this is true.

19 What is the best way to give them security?
20 And so multiple choice. Answer A is strong
21 cryptography, and that, of course, is my favorite as a
22 cryptographer. This is what I really want to believe.

23 And number B is laws that guarantee
24 nonrepudiation. We have heard occasionally about
25 nonrepudiation. Russell mentioned it. Nonrepudiation

1 means that -- Michael, maybe you can define it better
2 than I could.

3 MR. BAUM: Sure, Carl.

4 There's the notion of nonrepudiation. It's
5 sort of a legal term, but the notion there would be
6 that -- and by the way I -- with full knowledge I'm
7 being set up for Carl. I will blissfully participate
8 in this exercise.

9 Basically what nonrepudiation -- the notion of
10 it there is that your transactions that you create will
11 be -- you have a high degree of confidence that they
12 will be enforceable. Okay. And one notion -- in fact,
13 the first use of that term in the context of even the
14 predecessors to electronic commerce, was actually by
15 security experts with no legal backgrounds. And they
16 basically presented it as though there is
17 nonrepudiation or there is not nonrepudiation, and they
18 presented it as a security service. The better way,
19 perhaps, to look at it was that systems would to a
20 greater extent or to a lesser extent support the
21 security service of nonrepudiation in that it would
22 give you some level of evidence.

23 Now, where I think Carl is going is talking
24 about future jurisdictions that have passed laws that
25 set up very strong presumptions that if you use a given

1 system, and if a given digital signature is received by
2 the recipient that, in fact, the originator, subject to
3 a number of conditions, would be held to have sent that
4 transaction. That is where it is. Now Carl, since
5 I've greased the slides, go for it.

6 MR. ELLISON: Thank you, very much. I should
7 mention that you're on a panel with me every time I
8 talk. And the third option is laws guaranteeing
9 repudiation. I had to throw that in, right?

10 How many vote for A? One. Only one?

11 How many vote for B? One, two, three, four.

12 How many vote for C? One, two, three.

13 MR. MEDINE: How about none of the above?

14 MR. ELLISON: None?

15 MR. MEDINE: None of the above.

16 MR. ELLISON: No. I didn't give you that
17 choice. I mean, I have spent my entire life in school
18 with multiple guess questions where I wasn't given
19 fourth choice. I'm not going to give it to you.

20 So I'm voting for C, and the reason I'm voting
21 for C -- I had this discussion with a few people
22 upstairs -- the trick here, the thing that
23 disillusioned me when I first got into E-commerce when
24 I was at Cybercash and for that matter the reason that
25 I'm now with Intel is that what we found out was that

1 consumers don't want securities the way cryptograms
2 define security. As Michael has said, nonrepudiation
3 was a term that came out of the cryptographic
4 community, and it was a term that I heard bandied about
5 by noncryptographers. And it's a case that the
6 cryptographers should have kept their mouths
7 shut, I believe, because, what we really discovered was
8 what consumers want is power over their own money.

9 They want control. They don't want security the
10 way a cryptographer defines security. Absolute privacy
11 or as close to absolute privacy as you can get,
12 confidentiality. The kinds of things that we
13 worry about when we design systems that could be good
14 enough to control nuclear weapons, the things we worry
15 about are not what the consumer wants.

16 The consumer wants the ability to control his
17 own property. And he's got that ability already, with
18 credit cards he's got it in reg E and reg Z and reg
19 E and reg Z are answer C up here. This is a
20 regulation that allows the consumer to say, no, I
21 didn't buy that. It allows the consumer to repudiate
22 some action, and to me as a cryptographer, I wanted A
23 myself.

24 My community of cryptographers encrypted the
25 discussion around B, so that would have been my second

1 guess. So what I learned from the consumers, from the
2 world, was that the answer was C.

3 MR. MEDINE: Thank you, very much, Carl. We have
4 now have had our hopes raised and our hopes dashed by PKI.
5 But we'll have perhaps a later discussion to clarify that.

6 I just want to mention that Hannah Stires is
7 here as well from the business practices, and she
8 and John have been integral in bringing together this
9 two-day event. I want to recognize their work and move
10 on to James Wayman, who is the director of the U.S.
11 National Biometric Center. So we can get an idea of a
12 way to authenticate.

13 MR. WAYMAN: Thank you. I appreciate that.
14 Can we have the slides? It's listed under -- Wayman 99
15 is the name of the file.

16 I'm Jim Wayman. I'm a director of the U.S.
17 Director of U.S. Biometric Test Center. We are
18 financed by the federal government to study federal
19 applications and state applications, too, of a
20 biometric identification.

21 We advise on the performance and design of
22 government systems, so we stay out entirely of the
23 commercial arena. We don't get involved in how
24 biometrics may or may not be used in commerce, nor do
25 we get involved in how biometrics may or may not be

1 used by individuals.

2 So when John Smollen called me up and said
3 would you be interested in doing the conference? I
4 said, I have to tell you, this is really beyond the
5 scope of what we're involved in, but nonetheless I
6 thought I would come and lend my two cents worth,
7 because I do know something perhaps about the area of
8 biometrics, if not this particular application.

9 There is a federal government interest site,
10 funded by both the DOD and the MIST, that's
11 www.biometrics.org. If you go there, you may have to
12 click a couple of times, but you will get to the
13 National Tester Center. And I'll get to our web page,
14 and you can see the kinds of work that we've done,
15 primarily in the area of the mathematical and
16 statistical evaluation of test results and system
17 performance prediction.

18 Next slide, please.

19 If we're going to be talking about biometrics,
20 we need to supply a precise definition of what we are
21 talking about, so we used this one, the biometric
22 identification is the automatic identification or
23 identity verification of individuals based on
24 behavioral and physiological characteristics.

25 By automatic, we mean that this identification

1 always occurs using a computer and in real time. You
2 may be interested in DNA analysis, but we are not. DNA
3 analysis is a laboratory technique. It involves human
4 intervention. It's not done automatically. It's done
5 in real time, so I don't know anything about it at all.

6 I'll talk in a minute about the difference in
7 identification and identity verification. But if
8 individuals -- I've left out the word living
9 individuals. We presume you have a living individual
10 in front of you. We're not interested in
11 identification of dead bodies or anything like that.
12 Those are forensic applications of human
13 identification.

14 Human identification being the super set of
15 biometric identification, which is a very small part of
16 human identification based on behavior and
17 physiological characteristics. We came to the
18 understanding a couple of years ago that even your
19 fingerprints are a function of your behavior. You
20 have to take a fingerprint, and you have to put it to
21 a sensor. And the pressure that you put on a fingerprint
22 and the amount of a roll or yawl or pitch that you
23 put on that finger really affect the image that comes
24 out.

25 You might think of your face as being a

1 physiological structure, but your behavior, as you
2 know, greatly influences the face that you present to a
3 sensor. So we know that all biometric devices operate
4 on the basis of both behavior and physiological
5 characteristics.

6 Next slide, please.

7 Now, what I found intriguing about Michael
8 Baum's presentation is that he talked about the two
9 ways that you can use this asymmetric public, private
10 key pairs. You can run them forward or you can run
11 them backwards. You can run them forwards by
12 encrypting with a public key, and therefore the
13 receiving with his own private key can decrypt the
14 message, and you can have secure communication.

15 You can run the key pair backwards, and you
16 can encrypt with the private key and use it as a
17 digital signature.

18 Well, biometrics works kind of the same way.
19 You can run these things forwards or you can run them
20 backwards. There's two ways, different ways, of looking
21 at this thing. You can use them for positive
22 identification to prove I am who I say I am. At least
23 this is with respect to a roll identity on the data
24 base or you can run these things backwards to prove I'm
25 not who I say I'm not.

1 The purpose of positive identification is to
2 prevent multiple users of a single identity. I would
3 think that in electronic commerce, that's primarily
4 what you're trying to do. You're trying to prevent
5 someone else from using my identity in a commercial
6 transaction. But what we kind of really fear is
7 biometrics thrown in the reverse and negative
8 identification to prove that I am not who I say am not.

9 Now, believe it or not, a negative performs
10 the largest form of biometric identification in use in
11 the world. In the State of California where I live,
12 you have to give a right thumb print to get a driver's
13 license.

14 The purpose of that is to prove that you are
15 not anyone who has previously had a driver's license in
16 the State of California under another identity. The
17 purpose of negative identification is to prevent
18 multiple identities of a single user. To prevent me
19 from getting multiple licenses in the State of
20 California under multiple identities to prevent welfare
21 multiple recipients receiving multiple benefits under
22 multiple identities, to prove I am not who I say I am
23 not.

24 I want to add one more thing about positive
25 identification, and that is ultimately biometric

1 identification can never establish who I really am,
2 only that I'm not the same person that presented myself
3 earlier on for enrollment. How do I really establish
4 -- I had a lie detector test once. And they kept
5 asking me if my name was Jim Wayman, and after a while
6 I started to think, how do I really know that my name
7 is that. I don't remember that. I don't remember
8 being born. That's the name that I've always gone by.
9 So ultimately there's a systemological problem of how
10 do we finally prove that we are who we say we are?

11 Biometrics cannot do that for you. It cannot
12 get you over that systemological problem, but what it
13 can do is say the person I see here before me today,
14 the person whose image I have, is the same person who
15 enrolled with this image earlier on.

16 I love the concept of truth versus fact.
17 Truth, you are maturing daily as a unique soul in the
18 universe. This I think is a religious statement. This
19 is a religious truth that I personally live my life by,
20 but, of course, religious truth is intruded on by fact,
21 and the fact with regard to biometric technology is
22 that my extracted biometric features are aging and
23 wandering all over and on top of those of other. As I
24 grow and age and change even on a daily diurnal basis,
25 my biometric measures change.

1 You know that your height changes during the day. I
2 guess they say you're tallest when you first wake up.
3 Your weight certainly changes as your hydration state
4 changes during the day. Everything about you changes
5 during the day. And one of the problems about biometric
6 measures is that they are not very repeatable, and they
7 are not very distinct. You object to that. You say
8 Jim, for crying out loud, I have read so many murder
9 mysteries, I know that fingerprints never change.

10 Can we have the next slide.

11 Well, here is the same fingerprint taken off
12 an individual at an interval of less than six weeks. I
13 don't know which fingerprint was taken first. I think
14 the one on the right was. About -- I might add that
15 we've tested about a dozen of the biggest and best
16 fingerprint algorithms in the world. None of those
17 algorithms have been able to successfully detect that
18 these two fingers match. About 3 percent of the
19 fingerprints that we've collected in our standardized
20 test data base -- we've got about 3,000 fingerprints
21 -- about 3 percent have levels of destruction
22 comparable to this one, and they cannot be matched by
23 even the best systems in the world.

24 The fingerprint that you see on the right is
25 a little bit over moist. It's a little bit too dark in

1 some areas, and there is some blurring of the ridges.
2 The valleys seem to be gone. The one on the left is a
3 much better quality image, but the fingerprint itself
4 is kind of gnarled, chapped and scraped and broken. So
5 you can see that your fingerprints aren't necessarily
6 repeatable. So I learned a new word this morning.
7 Maybe you did too. That is this GUID, was that the
8 global universal identification? If you are
9 looking to biometrics to supply the magic GUID, global
10 universal identification, it's just not going to happen

11 That's not what these devices are going to be
12 used for, because you enroll with the fingerprint on
13 the right, and then you come along and you present the
14 fingerprint on the left. And there is no system
15 currently in the world that recognizes those two prints
16 are precisely that same from the same individual, same
17 finger.

18 MR. MEDINE: Some people call it a GUID.

19 MR. WAYMAN: GUID? Is that what it is? That
20 was a new word for me.

21 I thought I'd contrast for a little bit the
22 difference between PINs, ID numbers, keys, and then
23 biometrics on the next session. I certainly am not an
24 expert on the first three, but it occurred to me that
25 PINs are fairly stable. My PIN for my phone at work is

1 1234. I suppose that is not a very good PIN, but it
2 has stayed that way, and it has not changed. You saw
3 my fingerprint changed. My PIN never changes unless I
4 change it. Unless I step in and intervene, my PIN
5 remains stable. My PIN is replaceable. If I lose it,
6 it gets compromised, I can just change it. If I get
7 worried you're going to call up and start getting voice
8 messages off my machine, I'll just go back and change
9 that PIN. It is certainly is interceptible.

10 In fact, I just transmitted it in such a way
11 that all of you intercepted it. But the PIN is primarily
12 linked to the account. In fact, a woman that works with
13 me as the administrator of the test center uses the PIN.
14 She has it.

15 So it doesn't identify that I'm the one
16 accessing the phone. She, in fact, would be accessing
17 the phone, but it's a link to that phone account. That
18 phone can be accessed by anyone who know the PIN is
19 1234. Only limited storage is required. If I forget
20 it, I can write it down on a piece of paper, four
21 digits, no big problem.

22 I guess you can you do that with -- I think in
23 FAST. You can't do it with one byte, but you can do it
24 with one byte and an extra bit. So the very limited
25 storage required for a PIN. ID numbers. You can add

1 -- unique to the ID numbers -- what I might have said
2 is that 1234 isn't very unique and if I probably asked
3 around here, some of you in this room are using that
4 same PIN for access to your account. So PINs are
5 certainly not unique, but ID numbers can be.

6 In fact, my Visa card's number, which I won't
7 give you, is unique. I've never had my Visa bill,
8 unfortunately, sent to anyone else, nor have I ever
9 received the Visa bill of anyone else. My Visa number
10 is absolutely unique, and you can say all the other
11 things about PINs apply to ID numbers. That's stable.
12 My Visa number doesn't change unless I change it. It's
13 interceptible. It's linked to the accounts. My wife
14 uses my Visa number whenever she wants to. It requires
15 more storage certainly than four numbers.

16 Now, the private key we've been talking about
17 in an asymmetric system, we can add maybe nonrefutable.
18 I can refute that I used the PIN. Oh, no. It was the
19 office manager that used the PIN, and that would be
20 true.

21 You might say it's nonrefutable. At least we
22 know that that message was generated from that machine
23 that held that private key. I may not know, as Carl
24 mentioned who was running the machine, who pulled the
25 handle, but at least I know that it came out of that

1 machine. And key isn't interceptible, because at least
2 once you've transferred the key to the machine in
3 question, the key doesn't pass around. You don't pass
4 that key around. It sits in the machine.

5 So those, at least, are my idea of what PINs,
6 ID and keys do for you, but on the next slide I'll show
7 what I think biometrics does for you. Biometrics are
8 unstable. My PIN, 1234, doesn't change, but certainly
9 my fingerprint does. My face print does. My hand
10 geometry does. It's nonreplaceable. If I lose or
11 compromise my fingerprint, there's nothing we can do
12 about that. I don't worry about that. If you look at
13 our web site, you'll find my hand geometry template on
14 there. You'll find a template from my right index
15 finger, and you'll also find my facial image, but I
16 don't worry about losing them too much, but on the
17 other hand if I did lose them, they're not replaceable.
18 I can get a new credit card number. I can't get a new
19 fingerprint.

20 Nonunique. Boy, you know, we all want to
21 believe we are unique, and I believe that as a
22 religious statement, but in terms of our biometric
23 patterns, roughly -- and it depends on how you set the
24 threshold -- but roughly three, four, five, six out of
25 a six out of a thousand people share your hand

1 geometry, close enough at least. So your hand geometry
2 is not terribly unique. A fingerprint -- some of the
3 good systems do pretty well. We've done 16 million
4 comparisons with only a couple of false matches.

5 One thing is interesting. There's a whole lot
6 of people who have fingerprints that match fingers --
7 other fingerprints on their own hand. And maybe -- my
8 rough guess is maybe one out of every 300 people have
9 two fingers that match each other very, very well, at
10 least by the standards of these automatic
11 identification systems.

12 So you might try that next time you see a
13 demonstration. You might see if can't fool the system
14 into thinking that one of your fingers is another
15 finger. That's a fairly common thing that happens.

16 Biometrics are interceptible. We don't see.
17 I don't know understand this model that some have
18 proposed that we're going to somehow have these
19 biometric templates flashing around on the internet. I
20 still haven't gotten that together.

21 People say we can encrypt the biometric
22 template. It seems to me that's just adding another
23 layer of indirection, and I really don't get that
24 either. I don't think biometrics are going to be --
25 you said it was a GUID. They're not going to be our

1 GUID. We're not going to have these things flashing
2 around on the internet. That makes absolutely no
3 sense, because they can be interceptible, and if they
4 are nonunique, they certainly can be refuted.

5 Now, there are a couple of things that are
6 nice about them, however, and that is that they're
7 linked directly to the person. If a person gives you a
8 fingerprint and if this one here, you know if the
9 person is me, it links the transaction to me. It
10 doesn't link it to the computer that held the key, for
11 instance, and lastly, the convenience of this. No
12 storage is required. I can give a fairly detailed
13 pattern on the face or my hand or my fingerprint or my
14 eye patterns without requiring any further storage.

15 Next slide.

16 Well, is there, then, a use for biometrics in
17 E-commerce, and I believe there is. And that's exactly
18 what Carl talked about. You can take your computer,
19 and you can lock it up in a safe. The other thing that
20 you could do and is being done and is commercially
21 available now is you can lock your computer up using
22 biometric access. So your computer holds your private
23 key.

24 Now, you don't know, perhaps, who is going to
25 get on your computer. I keep my computer with me all

1 the time. At least I try pretty much to, and I figure
2 if I ever let it down, it will probably be stolen. But
3 there are methods by which that computer can be locked
4 up so that no one but me presenting a correct biometric
5 measure can get on that, on the computer.

6 Such methods are available commercially now,
7 but authentication will be here on the commercial
8 level. I'm authenticating to myself to my own
9 computer, saying computer, you know me. I'm your
10 owner. You can go ahead and release documents signed
11 with my private key. So I release using the private
12 key using authentication on my own computer or you
13 might argue on your own local network. You might have
14 some sort of a local network in your office where the
15 biometric templates are stored at a local network level
16 and signed on biometric authentication.

17 I have no trouble with that, but I'd like to
18 see authentication at the user's option. I don't
19 currently use biometric authentication to lock up my
20 computer. I have that capability. In fact, there are
21 -- you can download a voice recognition algorithm for
22 19.95 off the internet from Tianetics, for instance
23 that will work right in your computer. It works on one
24 of our computers in the lab. You can try that out if
25 you want. At your discretion, at your option, you can

1 currently now, with existing technology, lock up your
2 computer using a biometric signal so that only you can
3 get on that computer.

4 You have control of the stored pattern. That
5 stored pattern that represents my fingerprint or my
6 voice print or my eye print sits only on my computer.
7 It never leaves my computer.

8 There's a second model people now are talking
9 about, and I believe that is going to happen in the
10 next couple of years because I've seen all the hardware
11 required. People are talking about embedding finger
12 print scanners in the smart cards so that the smart
13 card won't unlock whatever keys it holds until the
14 correct fingerprint is scanned on the smart card. I
15 believe that's a reality. I have seen enough hardware
16 now that I -- and I've seen some prototype devices.
17 And I think we're going to see fingerprint scanners
18 embedded into smart cards.

19 So you've got the fingerprint templates
20 stored on the card. You hold the card. The template
21 never leaves the card. You have total control over
22 your biometric measure.

23 Now, as you saw earlier on the slide with the
24 fingerprint that was all beat up, sometimes these
25 methods aren't going to work. So you have to install

1 a back door. In the case of fingerprinting, unless
2 you're a portion of the population, maybe a percent or
3 two that simply has such poor fingerprints chronically
4 that you can't use fingerprinting, what we generally
5 do is advise you to store two fingerprints.

6 And, see, your back door is the second fingerprint.
7 If your right index finger doesn't work, use your left
8 index finger. But in any case, there will be days when
9 you simply are not yourself, and the back door is
10 required to access to your equipment. So some of the
11 computer makers that are talking about installing
12 biometric devices at the bi-house level are also
13 talking about installing back doors. Complicated back
14 doors that prevents a thief from stealing your computer
15 and going in the backdoor, but backdoors nonetheless
16 that allow you onto the computer in the event that the
17 biometric device does fail and biometric identification
18 does indeed fail.

19 So consequently, I'm suggesting no mandated
20 standards or controls. Why should the government care
21 if I choose or not choose to lock up my computer
22 using biometric authentication. And why not simply let
23 the marketplace work this out or let the individual
24 users work this out or let me decide which level
25 of security I want controlling access to my

1 own computer. I can imagine some liability issues
2 where you say to people, well, if you lock up your
3 computer with a biometric access control device, we
4 won't hold you liable for any charges that are incurred
5 by unauthorized use of the private key for instance. I
6 can see us doing that, but I don't understand the need
7 for mandated government standards if we're only talking
8 about access to my computer. And currently available
9 technology is that we had to do this.

10 There are fingerprint devices that are being
11 sold now embedded into keyboards. There are facial
12 recognition devices that you can download from the
13 internet, and pay, I believe, it was \$135 for it last
14 time I saw it. Now, for facial recognition devices,
15 obviously your computer is going to need a digital
16 camera, but I've been told by computer manufacturers
17 that they expect most computers to come with digital
18 cameras here in the near future. You can download the
19 Tianetics piece of software for voice control at your
20 computer using the built-in microphone that your
21 computer probably already has. So these devices are
22 already currently available.

23 So if you feel the need to control access to
24 your computer using biometric devices, the technology is
25 already in place. You can do that, and I'm suggesting

1 no further need for standards or mandated
2 regulations.

3 MR. MEDINE: Thank you very much. Thank you
4 for all of your presentations. We will take a
5 ten-minute break, and resume at about ten of 4:00.

6 (A recess was taken.)

7 MR. MEDINE: Okay. Thank you. Why don't we
8 resume? Now the hard core of the hard core are here.
9 Um, I'd like to first ask -- I've been asked to
10 identify -- that everybody for the benefit of the court
11 reporter talk more slowly, which will be a major
12 challenge.

13 I would like to start off with Margo Saunders
14 and ask her to give some perspective on some of the
15 discussions that we've just heard.

16 MS. SAUNDERS: I think the issue of when
17 digital signatures were necessary or when
18 authentication is necessary should really be enhanced
19 by looking at the authentication rules that we have in
20 common law in the real world and then see how those
21 rules are changed when we enter into the virtual world.

22 Basic contract law says that an oral contract
23 is just as valid as a written contract. The problem
24 only becomes proof. And it's obviously easier to prove
25 the terms of a written contract than it is an oral

1 contract. When that rule becomes changed, state law
2 in almost every state law are when -- generally when
3 the transaction involves either a large amount or an
4 issue of such importance that the law has said we must
5 have the contract to be written, otherwise
6 regardless of the ability to prove its terms, it will
7 not be enforceable.

8 An example of that is a real estate contract.
9 Both parties may totally agree that the terms of a real
10 estate contract are the same, but the law will not
11 enforce it unless it's been in writing.

12 The standard is the statute of frauds. The
13 statute of frauds requirement in most states say no
14 contract can be enforced for a value of more than \$500
15 unless it's in writing. And then you go on to parole
16 evidence rules. You have authentication requirements,
17 evidentiary rules when you are trying to prove
18 something in court and so on and so on. What happens
19 to, say, the statute of frauds when you have an
20 electronic transaction?

21 The issue as to the validity of the terms of
22 the contract when the entire transaction is
23 electronically -- is conversed electronically becomes
24 are the parties who they say they are? And is the
25 terms of the contract as reflected in the electronic

1 reproduction reasonably reliable? And it is that type
2 of analysis I think that we get into before we even
3 need to talk about do we need a digital signature. I
4 don't need, and I don't think I'll ever need, a digital
5 signature for my e-mail with my office, which we have
6 quite a bit. We have a Boston office, and we probably
7 exchange a hundred e-mails a day, and we don't need
8 digital signatures. But if I decide to buy some land
9 in Montana, and I promise that Margo Saunders will pay
10 \$20,000 for these ten acres of land in Montana, I sure
11 as heck want the person on the other end to know that
12 they are really dealing with me, Margo Saunders, and not
13 allow David Medine to promise that Margo Saunders is
14 buying the 20 acres of land in Montana.

15 Now, I also don't need a digital signature so
16 long as I'm using my Visa or my MasterCard, because
17 under reg Z, I have the protections of the Billing
18 Rights Act, and that law is not perfect, but it
19 provides virtual protection so as long as within 60
20 days after I get my bill if I recognize that there's
21 some mistake on it that I follow the rules. But that
22 is about it so far as consumer protections in federal,
23 and there's virtually none in state law.

24 So if I were to use my Visa, my other card in my
25 wallet, which looks like a Visa, but is actually an ATM

1 card, and buy a book through Amazon.com and actually,
2 and it's never delivered. I do not have nearly the
3 degree of protection under reg E that I have under
4 reg Z.

5 Now, I cannot complain that the book that was
6 delivered that I was promised, as I can under reg Z.
7 I can only complain that the amount that I authorized
8 to be withdrawn was not withdrawn. And I have a much
9 smaller amount of time within which to complain, and I
10 have the burden of proof and the money is taken right
11 out of my checking account for whatever account, the
12 ATM card is tied to, and it stays out until I prove
13 that, in fact, that I did not authorize that
14 transaction.

15 So when we talk about authentication, and we
16 talk about the degree of whether we're doing digital
17 signatures or PKIs technology or biometrics. It all
18 depends on what the purpose of the authentication is.
19 And I think it's very important -- I think the
20 underlying assumption has to be that we have built an
21 entire system of commerce using credit cards that have
22 just taken off that is based on a repudiation to use
23 Carl's analogies. It's an ability to repudiate an
24 improper transaction, and I don't believe that we will
25 have a similar take off of jump start of internet

1 electronic transactions until consumers have the
2 ability to repudiate transactions that both either were
3 not really theirs or were not really according to the
4 terms that they thought that they agreed to.

5 MR. MEDINE: Let me just pose that question to
6 Russ, which is as Margo says, we have existing
7 protections under Unfair Billings Act and regulation Z
8 against improper use of credit cards. Why do we need
9 SET? Why do we need digital signatures from the
10 consumer's perspective if they already have those
11 protections.

12 MR. SCHRADER: Well, I have good news for
13 Margo. Provided that you used your ATM card, and it
14 was a Visa, it was a Visa ATM card, on-line Visa debit
15 card, you're covered.

16 Last year Visa adopted the zero liability
17 policy. If there's unauthorized charges within the two
18 first days, you have zero liability. Although you
19 don't have regulation Z protections, you have the
20 voluntary protections that Visa implemented called
21 charge-back mechanisms. If that's not your book from
22 Amazon or if it's defective charge, return it. That
23 institutes the charge-back, and it will be handled
24 through Visa's charge-back system. If you have a card
25 that doesn't say Visa, well, shame on you.

1 MS. SAUNDERS: May I respond to that?

2 MR. MEDINE: Yes.

3 MS. SAUNDERS: The National Consumer Law
4 Center receives from legal services and private
5 attorneys all over the country, and when it's an
6 electronic issue, it's generally referred to me. I get
7 many, many calls who have done their homework, and
8 they've read reg Z, and they've read reg E, and
9 they've done everything that they reasonably can have
10 done. And they have not been able to find in any of
11 the law books that they know of any mention of a charge-
12 back. But they still are having a problem with the
13 bank, and they've got a client who has had this
14 problem, and this is great and wonderful because Visa
15 and MasterCard -- because MasterCard is willing to do
16 this, but it won't work until it's in the law.
17 Otherwise, I'll keep getting these calls.

18 MR. SCHRADER: Clearly I can't speak to the
19 charge-back policy, is it in reg E or reg Z. It is
20 in the Visa operating regulations, and the attorneys
21 that are calling you should frankly be calling the
22 issuer banks, and say, look at your Visa operating
23 regs. That's where it runs through, and there is a
24 zero liability on debit cards, and they absolutely
25 should be taken at the issuer. If it isn't there and

1 the issuers don't succeed in following the op regs,
2 then Visa wants to know about it so that they can look
3 at it, but clearly it is part of the contract that Visa
4 and the issuing banks, requires banks, and the
5 cardholder all vary.

6 MR. MEDINE: Can you just go back to my
7 question? Why do we need SET if we have from the
8 consumers' point of view if we have protections,
9 repudiation? Why do consumers need authentication,
10 encryption, digital signature technology if they have
11 legal protections in place?

12 MR. SCHRADER: They do have legal protections
13 in place. SET and all authentication issues, and I'm
14 not just going to say just SET, because we've heard
15 about a lot of other alternatives that could work
16 easily as well, SSL and the rest of it. It's one
17 additional layer to set the kind of environment that we
18 have that allows Visa to make the kind of promises. We
19 have been able to offer this kind after zero liability,
20 because fraud numbers have gone down. Fraud numbers
21 have gone down because of risk management tools,
22 because of authentication, because of encryption,
23 frankly, because of the help that the FTC has given
24 us, this going after the bad actors. We've been working
25 with your group as you know, in some of these web

1 merchants and shutting them down, and we appreciate
2 that help. That's allowed us to make these kinds of
3 market moves that has helped.

4 To continue to have authentication, whether
5 it's SET or SSL, other kinds of encryption, it will just
6 continue to make the environment more comfortable and
7 reduce the level of fraud.

8 MR. MEDINE: Mr. Ellison.

9 MR. TORRES: Actually, I just wanted to jump
10 in again, and I'll be talking a little bit about the
11 payment question. But just to get back to the idea of
12 debit cards and the voluntary liability and I think
13 there's a panel tomorrow talking about self regulation,
14 and I just kind of put that voluntary limits in it.
15 The consumers' union had been out there with the NCLC
16 and others and I think if Edward was here he would also
17 relate some stories about how there's apparently been a
18 failure in the way that voluntarily that program is
19 working and why in some cases we do need some regulations.

20 I don't think they are in question on using other
21 forums and why we need some of these other forums. If
22 we've got the limited liability on the credit cards,
23 there has been this push to use debit cards, then why
24 this push for this other technology, and what's behind
25 it, and how do we get consumers kind of geared up to

1 using those other technologies. If there is going to
2 be problems with liability and problems with security
3 and those other systems.

4 MR. ELLISON: Sure. This is -- maybe this is a
5 bit -- and it may turn a lot of people off, and if you
6 go to sleep through this, I'm sorry. Michael alluded
7 to this. Margo, at one point I love what you were
8 saying, but at one point you referred to knowing who
9 was making this transaction, this land purchase,
10 knowing that it really was Margo Saunders at the other
11 end of that wire and not someone just claiming to be.
12 And I think that's what we're talking about when we
13 talk about authentication.

14 The trouble is we are accustomed, and in a way
15 that law is accustomed to speaking of authentication
16 by talking about people's names. You used your own
17 name on that example. Michael was careful not to tie
18 all those to names.

19 The SET example was my favorite example. The
20 cardholder certificate on SET does not have the
21 person's name on it. It's an entirely anonymous
22 credential. It authorizes the key holder to use a
23 given credit card, but that's all it does.

24 So what I think is important here, one of the
25 things that happens with the internet that people don't

1 talk about very much -- I try to talk about it, and
2 Michael knows I talk about it so he set the stage for
3 that -- but one of the things that happened is that
4 suddenly we have a community that is so large that the
5 names we are used to using as identifiers don't work
6 anymore.

7 I went all the way through school as the only
8 Carl Ellison. So if someone wanted to refer to Carl
9 Ellison, I knew they were talking about me and so did
10 all my classmates, but I am far from the only Carl
11 Ellison on the internet.

12 My identifier is no longer a valid identifier,
13 because the community has gotten so big.

14 Now, if we make any rules or laws that have to
15 do with authentication, with identification of people,
16 and we refer to people by names, if we -- if the laws
17 say that the name of a person is somehow an identifier,
18 we're in big trouble, but then, any other kind of
19 identifier, a national ID number, for example, gets us
20 into a different kind of a trouble. This is a very --
21 it's a very horny issue, and it's something that we've
22 got to address; but I don't have magic answers for you.

23 MR. MEDINE: Margo?

24 MS. SAUNDERS: I'd like to respond. I think I
25 was using my name as a way of identifying me. And in

1 fact, the point I was trying to make is that sometimes
2 me, Margo Saunders of Virginia or Washington D.C.,
3 doesn't need to be identified on the internet. In
4 fact, perhaps I would prefer not to be identified, but
5 I may want to participate in some chat room, not
6 really, but I may want to -- someone might want to
7 participate in some chat room where it's a closed
8 group, and there might be some degree of testing or
9 something that people want to apply to the folks that
10 participate in it, but nobody needs to know and nobody
11 really wants their real name to be used.

12 So we might have a digital signature or some
13 kind of authentication technology that would be used
14 deliberately anonymously, but to apply to different
15 people. And then it would be totally different and
16 we would want a completely different authentication
17 technology and probably I might prefer this biometric
18 technology that would allow me, this Margo Saunders, to
19 buy land in Montana so that any other Margo Saunders --
20 and actually I have searched the net, and there isn't
21 any other Margo Saunders on the internet.

22 And that's why we don't want a national ID.
23 We don't want one authentication technology. We want a
24 whole series of them. And issues is: A, how reliable
25 they are, and B, who holds the purse strings if they

1 are proved wrong?

2 MR. ELLISON: I actually met someone who
3 provides an example of that chat room that you're
4 talking about, your hypothetical chat room. He runs an
5 on-line discussion group for incest survivors, and two
6 of the characteristics of this discussion group have to
7 be first of all complete anonymity because an
8 incest survivor is so sensitive, so fragile, that this
9 person will not open up and discuss it except under
10 strong anonymity. But you also have to have very
11 strong access control. You have to know that only
12 fellow incest survivors have access to this group for
13 this therapy group to proceed on-line. So that needed
14 is very strong anonymous access control.

15 MR. MEDINE: I'd just like to turn this
16 discussion around a little bit because we've talked on
17 this panel so far about identifying the individual.
18 What about using authentication to identify the
19 merchants? On the internet we tend to identify
20 merchants by a common name. Of course, someone else
21 might have gotten to the domain name first and pretend
22 to be a well known store.

23 Since we're trying to apply the technology to
24 electronic commerce, what do you think about using it
25 in a reverse way so that I as a consumer know that I'm

1 dealing with the off-line world merchants that I think
2 I've been dealing with or even on-line world merchants
3 that I've dealt with in the past.

4 MR. TORRES: I think absolutely. I was just
5 thinking fully it's a two-way street and I think
6 sometimes the consumer advocates and the industry folks
7 who have created this sometimes wonderful technology
8 above each other, but it really is a two-way street in
9 the same way that businesses and the service providers
10 want to authenticate who they're dealing with,
11 consumers need to know -- and I think it's even moving
12 beyond just what the OECD and other people have about,
13 you know, getting a name and address,
14 a way to contact the business with a proper telephone
15 number, but also to truly authenticate who the other
16 party is that you're dealing with on-line, and in the
17 same way you're talking certifying or authorities for
18 consumers, it's almost as though we need the consumer
19 thing for the business.

20 MR. MEDINE: Sure. Mike.

21 MR. BAUM: Sure. And as it turns out, for
22 example, our company, Verisign, has issued about
23 1,250-plus certificates to businesses to authenticate
24 their web sites, and we haven't seen any litigation
25 yet; and it seems to be working. And while, of course,

1 we can get into a thrash of precisely how we should
2 identify that person or what type of name structure we
3 should use, it seems to work.

4 You'll remember an interesting thing Carl said
5 a little while ago. He said, quote, there is no PKI.

6 Well, while certificates have not been widely
7 deployed for end-user consumers as of yet, from the
8 perspective of certificates issued by certification
9 authorities within globally deployed PKI, that's out
10 there, and what is interesting is if you think about
11 the number of actualness instances in which these
12 certificates or actually being used at this moment,
13 each of those certificates of every web site, so for
14 example, every time money is sent for example over
15 Amazon.com or for that matter some of the transactions
16 at Ebay or wherever else, the certificate is being used
17 to authenticate the web site to the user and to assure
18 a secure communication channel. That's not digital
19 signatures from the end-user consumer to the company,
20 but it certainly is an authentication mechanism. It
21 certainly is part of the broader global PKI that's
22 already been deployed, and it certainly has been of
23 great value to the enhancement of electronic commerce
24 generally.

25 MR. ELLISON: And yes, thanks for correcting,

1 Michael. I was a little sloppy when I said there is no
2 PKI. There is this existing set of certificates issued to
3 merchants for SSL purposes, and the browsers do check
4 those certificates.

5 I do have a complaint with the browsers, and
6 that is that the information that they check and
7 verify is not provided to the viewer. It's made
8 available on an option, but I don't know of anybody
9 except me who actually goes and looks. But that's not
10 the point I wanted to make.

11 David, you said that if someone might have
12 gotten a domain name for that well known name, IBM.dot.
13 They didn't get that name or they didn't get Intel.com.
14 For well known names, that's fine. These are names
15 that all of us agree on.

16 I assume everybody in this room would agree
17 that when I said Intel, you think of the same thing I
18 think of, but I don't think that's the issue with
19 electronic commerce and especially not global
20 electronic commerce. I think the issue is that we are
21 running into web sites we have never heard of.

22 You've never heard of this merchant. You will
23 never encounter this merchant physically, somebody
24 over -- Dorkmund, Germany, you're not going to run into
25 them on the way out of the door of this building. The

1 question I think we need to answer, and this was
2 addressed some in this morning's session, what happens
3 when you move to a new neighborhood, and you have to
4 decide what dry cleaner to use or where to do your
5 food shopping, what drug store to use.

6 You can go into a store and look around and
7 see how well kept it is, how efficient it seems to be.
8 You can talk to some of the sales personnel in the
9 store, or you can do what I do, which is talk to my
10 neighbors. I said, by the way, what is your dry
11 cleaner? Do you have a favorite doctor? I get
12 recommendations from people. That's the mechanism that
13 I believe we need the most, not just a mechanism that
14 securely attaches the real name of this merchant to his
15 web page. That's the mechanism that is proceeded today
16 by SSR certificates, but if I never knew that name, if
17 Hanz's Bakery in Dorkmund is unknown to me, the fact that
18 this web site came from Hanz's web site in Dorkmund
19 doesn't help me. What I want to know is how good is
20 their product. How good is their return policy? Do
21 they ever cheat their customers? That's the
22 information I need to know, and that's not being
23 provided here.

24 MR. MEDINE: And stay tuned for tomorrow's
25 discussion in the afternoon on seal programs as

1 potentially a start in that direction.

2 Mark, do you have a comment?

3 MR. BOHANNON: I was just going to --

4 MR. MEDINE: Can I just introduce you as Mark
5 Bohannon, who is the chief counsel for technology at
6 the Department of Commerce and just -- as you know from
7 this morning, has been very cooperative in helping us
8 put together this workshop.

9 MR. BOHANNON: I was just going to -- Carl
10 sort of jumped the gun, but I mean underneath the
11 rhetoric around the WIPO process to speed resolution is
12 the next very serious question that Carl raised in
13 making sure that you have confidence in who you're
14 dealing with, whether that's the owning of the domain
15 name or the web site or anything else.

16 I also think it raises a question that has not
17 gotten a lot of publicity, which I think is a good
18 example of the need for groups like the FTC to work
19 with their counterparts abroad to make sure there is
20 collaboration and effective implementation, and I would
21 bring to the attention of the group here that it was
22 your work with your counterpart in Australia that
23 recently settled the deception case about internet
24 Australia registering false domain names and
25 deceptively giving people dot-com, dot-net, dot-org.

1 It was the two of you working together with us and with
2 NSI that shut them down, made them pay a fine, and as
3 an example, I think, of the kind of cooperation we're
4 trying to get here.

5 MR. MEDINE: That's a nice transition into
6 talking about the international workshop ramifications
7 of authentication, which is, of course, what the
8 workshop is about. I was wondering if you could talk
9 briefly about where we are internationally in terms of
10 setting standards about what the laws are for both PKI
11 and other technologies.

12 MR. BOHANNON: Again, this workshop is
13 somewhat about international aspect, so I think I was
14 brought here as probably one of the few people here who
15 were working on this in an international context. Let
16 me preface my review with a couple of caveats and
17 observations.

18 Certainly I think it's clear from the
19 presentations today that both domestically and
20 internationally when you talk about electronic commerce
21 and transactions, consumers are a key part, but the
22 reality it that what we have dominating right now is
23 business to business transactions.

24 Naturally, that is therefore the dominant
25 discussion that is going on internationally.

1 Let me tell you how I think prevalent business
2 to business are. And it's an anecdote going back to
3 the discussions I was a part of almost a year ago when
4 the internet was trying to put together what it
5 believed would be internationally accepted principals
6 for government action on things like electronic
7 signatures. And we got into this discussion about
8 consumer activity on the internet versus business to
9 business, and so I finally just asked, and these were
10 people who are in the middle of engaging in this
11 internationally, what percentage of transactions and
12 what percent of business do you think on the internet
13 is being done on a business-to-business basis to
14 consumer.

15 Let me say that I was the conservative in the
16 room when I said 85 percent of all transactions. And I
17 think it was important to keep in mind that the fact
18 that most of us in this room deal with the internet in
19 that context of what you like to get off a web site,
20 that really is right now a very small part of what is
21 going on in the internet. So that when you're talking
22 about rules, when you're talking about electronic
23 authentication, you have to make sure that you're fully
24 aware of the picture.

25 There are a number of developments, and really

1 my goal here is just to provide you a summary of what I
2 believe is going on, but I think there is, in fact -- I
3 think you could divide the world into two different
4 spheres about how they are approaching the idea of
5 electronic authentication. And it really comes down to
6 whether a particular jurisdiction or a particular forum
7 is operating under what I would call the old
8 assumptions of the internet or I think the reality of
9 the internet.

10 The old assumptions in my view boil down to
11 the longstanding view that we were going to be dealing
12 with stranger-to-stranger transactions in primarily
13 open systems where we needed hierarchies and digital
14 signatures, that there were going to be very specific
15 business models in which this was going to be done.
16 And there needed to be a focus on the role of this
17 signature of the transaction to enable global
18 electronic commerce.

19 I think as the discussions here -- as I pointed
20 out, the reality is, in fact, very, very different than
21 those assumptions. That in fact what we have
22 dominating right now are commercial transactions
23 between commercial players that operated in either
24 technically closed operations or as Michael pointed out
25 in a graduation of closed systems based upon private

1 sector arrangements, whether those be by contract or
2 operating rules or other business practice. And then,
3 in fact, rather than a small number of business models,
4 we have quite a large number of diversity of business
5 models.

6 We were just at a workshop last week at
7 Stanford, sponsored by the Organization for Cooperation
8 -- Economic Cooperation and Development that we brought
9 together for two and a half days players from around
10 the world and everything from manufacturing and
11 financial services, entertainment was involved,
12 including even governments who were trying to use
13 electronic commerce to provide services.

14 What we saw really was a variety of approaches
15 both in technologies and in business models.

16 Finally, the final conclusion on sort of the
17 new realities or the actual reality of the internet is
18 that rather than trying to write new rules that we are
19 engaged, I think, in a more productive exercise to try
20 to look at applying existing rules that we all know
21 effectively into the on-line environment.

22 And that the focus is really on the
23 transaction and the context in which things are being
24 accomplished rather than a particular implementation
25 like a signature.

1 So with that in mind, let me try to describe
2 what I see as sort of in a commercial context the two
3 words that are dividing. I would say one-half of the
4 world represented, I think, by the United States, by
5 all Australia, by the United Kingdom, to some degree by
6 Japan, is really a very basic approach that says we
7 don't need to establish rules that guarantee a
8 particular standard or approach to electronic
9 authentication, rather we need to look at our legal
10 framework and make sure that if you do business
11 electronically, it is not discriminated against.

12 The activities that are engaged here are
13 basically based on the work of a group called the
14 United Nations Commission on International Trade Law,
15 which in 1996 produced a model law on electronic
16 commerce. It is focused on commercial transactions,
17 but with all its work, it could eventually be applied
18 in other areas, but the focus has been on commercial
19 transactions.

20 So in the United States we have activities
21 like the effort by the National Conference for
22 Commissioners of Uniform State Law to develop something
23 called the Uniform Commerce Transactions Act, which is
24 basically saying don't discriminate if you do work --
25 if you do business electronically. Get rid of the form

1 requirements which say that a record has to be in
2 written form or that a signature has to be in a written
3 form.

4 The second model -- and again, these are
5 rough; I'm just trying to give you an outline -- says
6 that you need the government to establish the rules of
7 the road, identify the standards, and in some cases
8 create certain presumptions for how electronic
9 authentication ought to be done. And with due respect
10 to people I know in the room, I think the classic model
11 for this is the European Union Signature Directive that
12 is currently underway and more specifically in the
13 German Digital Signature Law, which has been in effect.
14 And both of these say that it is the fold of government
15 to look at the standards, look at the basis on which
16 you accredit certificate authorities. In some cases
17 that gives a heightened presumption to the legal effect
18 of your transaction.

19 There might be places where the role of
20 private sector arrangements is respected, but it is
21 not, I would dare say, at the forefront of the concern.
22 I think the challenge that we have, and I can say this
23 both as my experience working both domestically and
24 internationally, is that the systems are not going to
25 change how they unfold.

1 I think the United States is going to proceed
2 as we are. I think that the many of the states in the
3 European Union are going to proceed as we are. I think
4 the challenge is trying to figure out how we make these
5 systems, how we build bridges between these systems. I
6 say that in the sense that it's going to be very
7 important in order to facilitate electronic commerce
8 that we have a common understanding of the goals, the
9 purposes, and the objectives of the systems.

10 And I think that what we're going to quickly
11 see unfold is, in fact, that many of the differences
12 are not per se about the technological implementations.
13 That there are, of course, always domestic concerns
14 about that, but that there are very different
15 approaches if you are a common law country versus a
16 civil law country. If you have a culture in which the
17 government has for many decades in some cases centuries
18 played a central role to making commercial transactions
19 or other kinds of transactions valid, that at some
20 level it's not about the electronic authentication that
21 is going to be the most difficult part. It is looking
22 at what are longstanding cultural and legal systems to
23 see how we can make them work more effectively together
24 given the global nature of the economy.

25 So with that I give you that overview, and to

1 emphasize that again most of what is going on
2 internationally right now is commercial, but consumers
3 do come into contact since consumers often rely on
4 those commercial parties in facilitating their
5 transactions abroad. Lord knows the last time I was in
6 Paris I was very lucky that a certain company's network
7 worked and that the contract between the merchant bank
8 that I was getting the money from worked and that the
9 system worked. So consumers are relevant, very
10 relevant to this discussion, but the international
11 issue right now I think is being focused on is the
12 commercial nature of these transactions.

13 MR. MEDINE: Thank you, Mark, for that
14 summary.

15 Margo, in your paper that you submitted, you
16 talked about an alternative to dealing with existing
17 infrastructures, which is the creation of a world
18 consumer organization. How do you see that playing
19 into setting the rules for authentication?

20 MS. SAUNDERS: There are a lot of other things
21 I wanted to say. Can I say those things and then
22 answer the question?

23 MR. MEDINE: Sure.

24 MS. SAUNDERS: I'll try to be brief. I think
25 there's very different -- there's quite obviously a very

1 diverse set of opinions here at this table, and I think
2 I would like to pose a question that you have not asked and
3 answer it. I a few of us, Frank and I particularly,
4 are very interested that you hear this point on this
5 issue.

6 The development of the Uniform Electronic
7 Transactions Act, which my friend from the Department
8 of Commerce has referred to, and similar laws on the
9 state level, has established a -- have been -- have
10 gone on with the basis of -- with the basis that most
11 transactions entered into between parties on the
12 internet are truly negotiable by both parties and that
13 both parties have equal bargaining power and equal
14 access to information and equal access to choices. And
15 that is certainly true in many situations in commerce.

16 The problem is that when you apply that basic
17 assumption to business versus consumer, now the beauty
18 of the internet is that presumably it opens up the
19 marketplace for all consumers and allows consumers to
20 shop or realistically much more broadly for whatever it
21 is that they're looking for. But the fact of the
22 matter is that every consumer in almost all situations
23 are not allowed to negotiate the terms of those
24 contracts with those businesses, and either they take
25 it or leave it.

1 There are adhesion contracts which they cannot
2 negotiate, so that when for example a large business
3 says you shall use this digital signature, this digital
4 certificate, this certification authority in order to
5 transact business with us, and we will rely on the
6 private key or the public key issue, the private key
7 technology provided by this certifications authority
8 when we accept your orders to make checks, have checks
9 written to someone else by land or whatever it is that
10 reg Z doesn't apply to, the consumer has to accept
11 that those rules or not do that, not do this. And the
12 consumer, most consumers in this country at least
13 transact business with most businesses with the
14 understanding that there are basic consumer protection
15 laws that stop unfair and deceptive and just plain
16 wrong behaviors, and generally there are. They're
17 state laws and federal law. There's generally federal
18 laws that prohibit that.

19 But what that means is that the lawyers that
20 Mark was referring to, you're assuming that those laws,
21 the electronic, state laws assume equal party
22 distinction between the people bargaining, and that's
23 wrong. And that means the consumers are going to be
24 left holding the bag when that certification authority
25 has made a mistake and has issued the certification for

1 this particular transaction which isn't valid.

2 MR. BOHANNON: I want to make sure we are
3 talking about the same thing, because I want to make
4 sure that, you heard me say when I was
5 talking about the Uniform Transaction Actions Act, I
6 clearly -- this administration and I will be absolutely
7 clear, is making absolutely no judgment about the
8 Uniform Computer Information Transactions Act, which I
9 think you were describing, which comes out of the
10 disaster of a disaster clearly.

11 So since we are almost in agreement, but I
12 want to be very clear that what I was describing it was
13 not USIDA (phonetic) it is the Uniform Electronic
14 Transactions Act, which the authors have meant to say
15 as in many of these cases is primarily about commercial
16 volume transactions and really deals with a very, very
17 simple proposition to enable electronic commerce.

18 It's not talking about the validity of the
19 contract, USIDA does. It's saying that putting the
20 validity question aside, making sure that there are not
21 written requirements that are discriminated against to
22 enable electronic transactions. It doesn't go to the
23 validity question at all. So I just want to make sure
24 that there is no confusion of what we are talking
25 about.

1 MR. MEDINE: I guess the question is should
2 there be a different set of rules for business-
3 to-business transactions where businesses can
4 negotiate at arm's length and set the terms, as opposed
5 to consumer-to-business transactions where consumers
6 typically don't get to negotiate those, and if that's
7 the case, why don't you try that in the international
8 marketplace?

9 MS. SAUNDERS: That's what I was getting back
10 to. Essentially there has got to be very different
11 rules and I think a whole panacea of consumer
12 protections that must be developed to deal with the
13 much more radically different in choice, in
14 sophistication, in bargaining power, in access to
15 information, that exists between consumers and
16 commercial parties on the internet. I think I've
17 talked enough, so I'll let you ask the question you
18 asked me, was something else, unless you want me to
19 answer it.

20 MR. TORRES: Here is the thing. I agree to
21 the extent that -- with what Margo said that to extent
22 that existing laws can apply that there is some
23 overlap. That's all well and good. It's always a bit
24 inconsistent to me that when I hear that, well,
25 because, you know, E-commerce really hasn't taken off

1 as much as business-to-business transactions have
2 occurred or because it's so new and people are just
3 getting into it, we really shouldn't have any
4 regulation, where at the same time it seems that like
5 that's always the case or self-regulation when it comes
6 to consumer concerns. But when businesses have a
7 concern, I'm certain that we've seen a full slate of
8 proposed legislation. You saw the UCC2B that has been
9 turned into this other monster come up. So it's just a
10 bit unassuming when you say any regulation is a bad
11 regulation. I don't think that's the case at all. I
12 think that in order for consumers to have confidence in
13 the internet, they need to be assured that some basic
14 elements are there.

15 If in the best of all worlds, it would be
16 great if we could rely on businesses to take it upon
17 themselves to say, look, we'll protect your privacy or
18 we will give you control over it. We will assure that
19 our site is secure, so that the information you provide
20 won't get into the hands of somebody who will use it to
21 take your identity.

22 We have -- to the extent that you are
23 purchasing a product from us, you will know what our
24 return policy is. You will know what it costs to
25 deliver it. Unfortunately, that's not happening. And

1 so, to the extent that it is, if I were -- I'm not in
2 business. If I were in business, I would say, fine.
3 Put in the protections, because I can adhere to that.
4 We don't want cumbersome, burdensome things. We're not
5 asking for that. But to me that helps the bakery in
6 Dusseldorf or whatever to actually compete with the
7 bigger players on the web, because the rules are the same,
8 and the consumer can say I can buy that pastry and have it
9 shipped to me overnight knowing that there are some
10 protections in place for me, that I don't have to rely
11 simply on the brand names that I feel comfortable with.

12 Because if you're solely relying on
13 the brand names that you feel comfortable with, then
14 the internet becomes kind of this novelty it's great to
15 kind of surf and get all this great information from,
16 but to really make E-commerce work, if you're just
17 going to the big brand names, is it really beneficial
18 to you? Are you really able to shop for the best
19 price? And so that's where the whole notion of having
20 another system come into play, because we are talking
21 about a multitude of jurisdictions. We are talking
22 about a lot of crossorder transactions with this thing.
23 It's going to work the way everybody says it is.

24 So the only thing that it -- I hate the
25 expression we have got to start thinking out of the

1 box, but if there's ever a time to do it, it's now
2 because the benefits are just tremendous from this
3 technology, absolutely tremendous, but everybody needs
4 to be good actors. We'll always have fraud. We'll
5 have bad actors. We'll have bad businesses. We'll
6 have consumers taking advantage of the system, but for
7 the people that really want to use it, let's set up a
8 system that benefits everyone.

9 MR. BAUM: I can agree so far as the notion
10 that, yeah, we need to start to think about this today.
11 Anyone that knows me probably knows I've been thinking
12 about it a long time, so I applaud that. And we should
13 be here today, and we should be engaged in precisely
14 this discussion. Having said that, I've got tremendous
15 concern about a knee-jerk reaction in this area.

16 First, we're not, at least in this panel at
17 least, I believe, talking about general consumer
18 protection on the web. Critical issue. Other panels
19 at this meeting. I thought we were here on the
20 authentication piece. So in terms of general consumer
21 protection, good practices and resolving many of the
22 type of, you know, nightmares that we heard upstairs,
23 my viewpoint on that is a separate issue than where I
24 want to go right now. On the authentication piece, I
25 think we really need to work with the following points.

1 The first one is notwithstanding at least the
2 hypothetical, if not on a practical level, the
3 potential harm that could come up with some scenarios,
4 I haven't seen as we've seen in congressional
5 testimony, the panel of victims. I don't see it yet,
6 and if it's not there, what's this notion about
7 short-term regulations?

8 Second point, the vast majority of the
9 transactions I've seen, and perhaps it's growing and
10 maybe Russ has something to say about it, is there are
11 being down with credit cards on the net. So you've
12 already got at least some of the better consumer
13 protection laws in place. This is nothing new.

14 So if that's the case and if that's the vast
15 majority of commerce, then what are we talking about in
16 terms of the regulations of authentication at this
17 early point when you're hearing about the biometrics
18 industry just starting up, the PKI industry just
19 starting up and other technologies and getting started
20 here.

21 Let's go beyond that. If you look at the
22 uniform electronic or strike that -- at least the
23 Bliley (phonetic) bill that I think I saw, there's
24 something out there in that regard, family law
25 transactions.

1 So one of the big problems we've seen, and I'm
2 sure the statute of frauds would cover chunks of this
3 anyway, is the short-term concern of the grandma losing
4 her house or her estate, may not be much more than a
5 sound bite at this point.

6 So let's really even go beyond that, since we
7 already opted out of the exception of the credit cards
8 and everything else that I, mentioned. So now we are
9 down to probably one of the killer applications that
10 we're going to see out there in terms of the broad
11 scale use, and it's really -- it was late in coming,
12 and the industry can be criticized for that. Others
13 can be criticized, but it is secure electronic mail.

14 So the extent that that's really going to be
15 the fantastic application to provide really hard-core
16 privacy between consumers with regard to their personal
17 confidential communications, including the
18 communication of credit card numbers, thank you very
19 much.

20 In that regard, again that goes back to the
21 type of model that I presented up there, this
22 nontransactional model, this is just direct
23 communications between two parties once they have some
24 types of authentication technology to use. And, of
25 course, PKI is a good one.

1 In any event in those types of transactions
2 we're not involved in, that's not even part of the
3 authentication per se.

4 Now, certainly you'd want to identify the
5 party on the other end, but even then, if you think
6 about what Carl mentioned about a group of -- what
7 kinds of survivors?

8 MR. ELLISON: That was incest survivors.

9 MR. BAUM: Incest. In that case, you may not
10 really care so much that the given person is a member
11 of that particular group, as you care that over the
12 course of time that you're communicating with members
13 of that group, that you're dealing with the same
14 person. So the notion of the importance of being able
15 to have assurances of the sequentiality of
16 communications may turn out to be a tremendously
17 valuable capability.

18 So where am I going? I'm trying to suggest
19 that the scope of applications, and by the way that
20 latter half didn't involve any money at all, by the
21 way. Of course, privacy and health information are
22 critical. The notion that I'm trying to raise is we're
23 just getting started here, folks. And the nature of
24 the actual risk, I think in actual terms of actual use,
25 may be different than what some people in this panel

1 are making it up to be today.

2 That doesn't mean we don't take seriously what
3 you're saying, but what it does mean is maybe the
4 following: We listen just as we are engaging,
5 but I truly believe for any type of viable
6 authentication laws have to come out that are going to
7 be broadly based, get uptake internationally, and, boy,
8 don't we know how important it is that we don't act
9 alone here in terms of having the scope of
10 international capability, but that's probably going to
11 take a few years of work. But to the extent again we
12 don't see the victims today, I strongly urge
13 that we don't have a knee-jerk reaction here, but we
14 methodically put good resources into thinking this
15 thing out and really take advantage of the
16 international forums that have already given this a lot
17 of thought.

18 MR. SCHRADER: I was a little bit concerned
19 about the international dimension and since it was
20 raised, I just want to address it.

21 I'm not sure that there is in any way an
22 agreement as to what international consumer protection
23 should look like. Example, the one that is
24 traditionally used is in France, they use a seven-day
25 cooling off period. In this country, I send to

1 Amazon.com, I want that book now. Tomorrow is too
2 late. I don't want it in seven days. You think about
3 sending it, Lord knows what kind of stale bakery I would
4 get from Germany.

5 In terms of the consequences, when you take
6 that in, I will submit it would be extraordinarily
7 difficult for a new business like Amazon.com to even
8 exist under that kind of a law.

9 The competitors where you can get your book
10 down the street and any place else that was not subject
11 to that kind of handling that was done in the name of
12 the consumer protection would stifle some of the unique
13 opportunities that has started to reform.

14 Once again, we talked a little bit about
15 contracts of adhesion, the take it or leave it aspect
16 of it. I don't know that it's any different where I'm
17 in a small town, and there's Walmart, and there's a
18 small hardware store. At this point in the internet, I
19 can tell them take it or leave it there and go to 27
20 different purveyors of CDs and tell them I'm going to
21 leave it because the 27th one has a little bit more
22 competitive advantage. That's where the competition
23 that we are trying to encourage comes from.

24 I think the private sector working through the
25 credit cards, that's tomorrow. I just want to talk a

1 little bit about the internet.

2 MR. BOHANNON: As I said, my expertise is more
3 in the commercial law area, but I hate to pick up
4 France again, but it's fun. For example, this is a
5 serious question that we are trying to address about
6 how to ensure effective confidence by consumers in
7 international transactions. For example, what do you
8 do with a situation where in France the fundamental
9 difference is even more than you talk about. In
10 France, there is nonrecourse banking. Well, there is
11 in the United States. In France -- well, I would say
12 most people in this room have a credit card issued by a
13 bank that is not where they do their traditional
14 banking. My guess, most of the people.

15 In France that's not the case. It is you get
16 your card issued by the bank you do business with.
17 That's affected the ability of many consumers in those
18 countries to be able to use the same rights that
19 consumers have here to say, look, I want to put a 60-
20 day hold. I want to have this investigated.

21 The question is not just about what you do
22 with a piece of plastic, and the rights that are a
23 associated with that. What we have are very
24 significant different traditions by which a variety of
25 consumers rights. And I agree we've got to figure out

1 some way to make it more transparent, to make it more
2 open, to understand how businesses can do.

3 I just have to wonder whether we will be
4 sitting here a hundred years from now with the same
5 panel with David and having the same discussion if we
6 try to talk about truly harmonizing consumer laws as
7 opposed to having them work in harmony. That's an
8 important distinction.

9 MR. BAUM: And I don't think either Margo or I
10 were implying that we should adopt the laws of France.
11 But at the same time, there is a lot of discussion
12 going on at the international level. I'm talking about
13 consumer protection and discussing things like
14 authentication, digital signatures, and how they apply
15 in the consumer's realm. I think they are important.
16 But, you know, we're not talking about adopting the
17 laws of France here.

18 MR. MEDINE: We have time for just a couple of
19 comments.

20 MR. ELLISON: Yeah. Michael reminded me of
21 just a couple more things that I like to point out.
22 I tend to think of transactions over the web being all
23 by credit card as Michael suggested, but they're not.
24 Intel does a huge amount of web transactions business
25 to business, and it's not by credit card. It's by

1 purchase order.

2 When I was back at Cybercash, we were worried
3 very much about how do we do electronic checking.
4 That's not credit card protected. Electronic use of
5 ATM cards unless the ATM card happens to have a Visa
6 logo is not credit card protected.

7 So it's not just credit cards. It would be
8 nice if it were in a sense. A little myth Michael. I
9 couldn't resist it. The secure electronic mail is not
10 that new. Anyone who has got my business card has my
11 got my PGP fingerprint. And that's been around since
12 1991. But the serious point is that I believe I agree
13 with Michael. We are here to talk about
14 authentication, but what's important to me is not to
15 use this authentication for the purpose of
16 identification, attaching a name or some other ID to a
17 key holder, because that assumes that I know how to
18 make use of that ID. You know, if I have somebody's
19 social security number attached to a key, heaven
20 forbid, that assumes that I know how to use that
21 number to look something up that is of interest to me.
22 What is important to me is that we have the
23 characteristics we care about, the attributes that are
24 important, attached to a key holder in some way that we
25 know is authentic. We know that these attributes were

1 signed into this certificate, attached to this key
2 holder by somebody who is trustily an authority on
3 those attributes.

4 If the attribute is my permission to use the
5 credit card because I've got a set card holder's
6 certificate, that certificate was issued by the issuing
7 bank. That's the true authority on this piece of
8 information. So I've identified a piece of information
9 I need to know about that key holder, namely permission
10 to use that credit card, and I've identified the true
11 authority for that kind of information, the issuing
12 bank.

13 Sure enough this piece of information comes to
14 me issued by that true authority. That's a
15 wonderful example. I worry about us not paying -- the
16 people who did SET spent a lot of time asking
17 themselves what is the important information and who is
18 the proper authority to issue this information.

19 What I worry is that we don't do that in other
20 things that we need to know. I worry when people talk
21 about authentication is just attaching an ID of some
22 form to a key and assuming, well, now we've done
23 that. We can go deal with other stuff, because that's
24 not the issue.

25 The ID is almost always useless because the

1 world is so big. We need to know what it is we want to
2 know about a key holder, and then for each of those
3 things we need to identify who is the authority.

4 MR. MEDINE: Margo, last comments.

5 MS. SAUNDERS: Michael is very worried that, I
6 assume, that the FTC is going to come out with a
7 recommendation that digital signatures and PKI
8 technology be regulated immediately by Congress.
9 Right?

10 I would not be at all dissatisfied if they
11 came out with that, although I would be very surprised.

12 I think where I am going, and I expect other
13 consumer advocates are going with this is that when
14 there is an independent certification authority that a
15 digital signature or some authentication technology
16 serves -- is to serve a particular purpose, whether it
17 is that I am Margo Saunders or that I am an appropriate
18 member of a particular chat room, anonymous as that may
19 be, or that I have the authority which may be from my
20 husband or from a friend or from a corporation, to use
21 a particular credit card, whatever the purpose is, if
22 the certification authority says that I am that person
23 with that authority, the question is, what is the
24 liability that attaches to the certification authority
25 if I am not that person, and if I have access and am

1 able to use that authentication technology
2 inappropriately?

3 And that's the regulatory question that I
4 think we need to answer. I envision a multiplicity of
5 authentication technologies for a huge variety of
6 reasons, because the last thing we're going to get in
7 this country, I hope, is a national ID.

8 We want for some transactions the anonymity
9 that the internet offers us, but we need somebody to
10 enforce, if it's not voluntarily enforced, the promises
11 that are made by the certification authorities,
12 whatever they are, and to hold the certification
13 authorities liable when those promises are not kept.
14 And individuals that and potentially businesses suffer
15 as a result. And that's the regulatory, at least, path
16 that I think we should be investigating.

17 MR. MEDINE: Thank your for provoking a lot of
18 good questions, and as with other subjects in this
19 two-day workshop, we do this as the beginning of the
20 debate and the discussions and not the end of it. And
21 I would like to thank you, all the panelists, for their
22 tremendous contributions. Thank you.

23 (At 4:52 p.m., the proceedings in the
24 above-entitled matter were concluded.)

25

1 C E R T I F I C A T I O N O F R E P O R T E R

2 DOCKET/FILE NUMBER: P994312

3 CASE TITLE: Global-E Marketplace

4 HEARING DATE: June 8, 1999

5

6

7

8 I HEREBY CERTIFY that the transcript contained
9 herein is a full and accurate transcript of the notes
10 taken by me at the hearing on the above cause before
11 the FEDERAL TRADE COMMISSION to the best of my
12 knowledge and belief.

13

14

DATED: June 21, 1999

15

16

17

LAUREL ALLEN

18

19

20 C E R T I F I C A T I O N O F P R O O F R E A D E R

21 I HEREBY CERTIFY that I proofread the transcript
22 for accuracy in spelling, hyphenation, punctuation and
23 format.

24

25

SARA J. VANCE