Montana Law Review

Volume 61
Issue 2 *Summer 2000*

Article 1

7-2000

Privacy in Cyberspace: Transcripts from the 1999 Judge James R. Browning Symposium

Jeff Renz
Introduction, jeff.renz@umontana.edu

James Harvey
Featured Speaker

PRIVACY IN CYBERSPACE[1]

Transcripts from the 1999 Judge James R. Browning Symposium

INTRODUCTION: ***Jeff Renz***

FEATURED SPEAKER: ***James Harvey***

MR. RENZ: . . . .

The subject of the next panel is cyber privacy, or privacy on the Internet.

To give you a feel for the framework of the discussion, our court and other courts have talked about privacy aside from the Internet and essentially broken it down into two spheres. The first . . . is transactional privacy; that is our right not to have other people or the government know what we happen to be engaging in at any particular moment. [The second is] . . . informational privacy; and that is our right to have other people or the government not know what it was we did the other day or collectively the last 365 days.

At some point, . . . transactional and informational privacy will overlap. On the Internet when we talk about transactional privacy, of course, we're talking about communications . . . .

. . . .

Currently, there is an Internet site, an Internet company called TRUSTe[2] . . . which gives out what they call trust marks. [TRUSTe] will certify that . . . [an] Internet site takes certain steps to protect your privacy interests.

The Internet industry is developing certain protocols to ensure privacy of transactions. Of course, we don't want our Social Security numbers or our credit card numbers handed over to anybody who might want to be able to find them. We want means to ensure that when we send that credit card number to

1. All footnotes are attributable to the editors.
2. <http://www.truste.org/>.

Montana Law Review, Vol. 61 [2000], Iss. 2, Art. 1

an E-commerce company, that that is the only place it will go to and not to other people, and that people will not be able to break into that company's records and pull that number and other numbers out.

So the tension here is between governmental regulation in order to ensure privacy, and governmental intervention in order to breach privacy, and the private sector's attempt to regulate itself and to ensure the privacy of its users.

. . . .

Jim Harvey is counsel at Alston and Bird[3] in Atlanta, Georgia . . . . [Mr. Harvey] concentrates his practice on technology and Internet-related transactions and advice. He's currently a member of the Board of Editors of *Computer Lawyer*, a member of the Computer Law and Intellectual Property sections of the State Bar of Georgia and [was] on the board of directors of the Southeastern Software Association . . . .

. . . .

I would like to welcome Jim Harvey who will give us a greater overview and certainly a more detailed one than I have.

MR. HARVEY: I'm pleased to be here in Missoula today. You have a lovely town. The Law Review has been quite accommodating and hospitable. The accommodations have been tremendous and everyone has paid a lot of attention and for that, the speakers, particularly the out-of-town speakers, are grateful. And I hope you enjoy the presentation.

As has been said, I'm going to give an Internet privacy primer . . . . I'm going to talk about what information is collected as you visit the Internet. Your click stream data. I will not talk about what happens when you fill out a bank application form or something like that. I'm going to focus my efforts directly on the information that companies and others are trying to cull from you while you are visiting the Internet.

I'm going to also give a whirlwind overview of the status of the [European Union] (EU) Data Directive[4] and U.S. policy with respect to the EU Data Directive . . . .

First of all, a commercial word from Alston & Bird. We have 450 lawyers in four offices; 130 lawyers in technology and intellectual property arena. We have a tremendous explosive growth in the Internet, E-commerce arena in our firm. The

3. Alston & Bird, LLP, Atlanta, Georgia. *See* <http://www.alstonbird.com>.

4. *See* James Harvey, *An Overview of the European Union's Personal Data Directive*, 15 NO. 10 COMPUTER LAW. 19 (1998).

reason I bring that up is I think it's reflective [of] why we're all here, of what's going on in society, and all that is wrapped around privacy and intellectual property.

My little world, my optic on this issue, is I have solely an Internet and E-commerce practice, representing companies in transactions with one another. Usually, due to the nature of the firm, I represent large companies. So I think it's important to convey to you the bias and what I do on a day-to-day basis. I am very much a working lawyer, not an academic. I have to write the contracts that deal with these issues, so that will, of course, flavor my comments.

What information is collected? As I said, I think it's important for us all to step back and think of your next Internet session or your last Internet session, what you did while you were there. Where did you come from? So if I'm CNN Interactive,[5] a client of our firm, or if I'm Yahoo[6] or Amazon,[7] whomever the case may be, they can generally tell what site you came from when you came to their site. That is incredibly valuable demographic information should they go out and cook up a deal with a certain sector of companies to try and encourage more eyeballs to come from that site to your site.

They can also tell the type of computer you are using. So are you on a 486; are you on a 586; are you on a Pentium; are you on an A and D chip? They can tell the size [of the] monitor, how many pixels there are in the monitor. They can change, dynamically generate web pages based on what they think is happening on the user's end of the screen.

They can tell the [Internet Protocol] (IP) address of the origin server. As you all know, a domain name is really a proxy, if you will. It is an easy-to-remember name which is a synonym for a nine-digit number that shows the computer by which you access the Internet. So that nine-digit number is called an IP address and your origin server is how you are hopping onto the Internet. They can tell the IP address of the origin server. Generally speaking, sophisticated sites can easily tell the IP address of origin servers of people hitting their site, particularly if they spend a long time there.

The other interesting thing about knowing the IP address is, are you coming from home or work? Well, interestingly,

5. <http://www.cnn.com>.
6. <http://www.yahoo.com>.
7. <http://www.amazon.com>.

Yahoo is the most traveled site from about 5:00P.M. until 11:00P.M. in the evening. During the daytime, the Netscape[8] site is the most traveled site. So there is a definite distinction in the way those entities want to portray their information, the audiences they are playing to, and they are culling all this as people visit their site.

. . . .

If you visit a site, generally sophisticated sites, in order to keep up with who is visiting their site and what they are doing while they are there, will put a small computer file, generally less than a 100K file, on your computer. You will never know it hit your computer. It's called a Cookie. And then the next time you come back to the site and they say, Oh, that's John Smith, that's Susan Smith. The last time they were here, they did this. They spent this long in the sports area; they spent this long in the health care area; they bought $300 worth of backpacking equipment, or whatever the case may be.

. . . .

More information is collected. What did you do while you were on the site? Again, think about your last or your next Internet session. Did you buy anything? It's a very simplistic statement, but if you bought pornography, clothes, backpacking equipment, a book on French literature or French wine, all that is getting dumped into a big database somewhere and they are not dumping it for no reason. Computer storage does not cost what it used to, but it costs something and that is very, very valuable information.

If you bank on the Internet—again, very simplistic, but think about it—they know how much money you have in your account, what your daily average balance was, [and] when the last time was you bounced a check. They may know your mortgage provider, et cetera. All this is going into databases and it makes for a very dynamic online environment.

Did you join a group? So if you went to a health care information site and you joined a group on gallbladder problems or arthritis, a pharmaceutical company will be extremely interested in those consumers out there that are trying to be educated, that are proactive. Internet users tend to have more money to spend, and they will be very interested in [whether] . . . you join[ed] the gallbladder group? Particularly if they sell a gallbladder medicine.

---

8. <http://www.netscape.com>.

So if you join a group while you are there and you disclose who you are in the process of joining that group, that goes somewhere.

What pages did you look at and for how long? Did you pause in the Missoula, Montana, travel section, or did you just zoom right out of that section and go to the Glacier National Park section? Again, very, very valuable information for the entities running these sites.

What did you say while you were there? This is what generally surprises audiences that I speak to more than anything. If you participate in list serves or news groups, most people think, okay, I'm going to say this, X, about Y topic, and that will go away in thirty days or whatever the case may be.

We have innumerable instances of litigation in our office that are based on evidence pulled out of archival databases where somebody said something in 1996 on a news group about some company and now they have gone back to the party hosting that news group server, looking for the archive, and that's being used in litigation. So if you are saying something and you are saying it in a public context, you need to think, this will probably be out there, more than in theory, for time immemorial.

What information did you volunteer? Again, another very, very simplistic point. But if Yahoo pops up a survey and says, "We would like you to tell us a little bit about yourself. What is your average yearly income? How many things have you bought the last year off of the Internet? What books do you read? What's your age? What are your main stock holdings?" You would be amazed at the number of people that will fill out [the survey]. If it pops up on the screen, they think it's true. Every one of these surveys that I've filled out, they all think that I make . . . a million dollars a year, that I'm twenty-eight years old, and I have this great stock portfolio, none of which is true. I am twenty-eight.

And where did you go when you left? So if you were at CNN Interactive and you went from CNN Interactive to Barnes and Noble,[9] which is one of their main partners, that is valuable information. If you went from CNN Interactive to WebMD,[10] which is a health care information technology company, that is also valuable information. Again, we know where they came

9. <http://www.bn.com>.
10. <http://www.webmd.com>.

from, we know where they went when they left. Let's go out and cook up a deal with these companies, maybe have a co-branded site, whatever, but all of this is going into the database.

The EU Data Directive.[11] It was effective in October of 1998 .... The EU Data Directive is the result of the European Commission, the EU, which you have all heard of.

Basically, the way the directives work in the EU is the Commission comes out with a directive that says each of the 15-member countries of the EU will adopt laws that say at least X, at least Y, et cetera. Then, ... in order to be acting members of the EU, the countries are required to adopt those laws, national laws. So rather than adopting a pan European law, the fact is [that] you have ... 15 different interpretations in three or four different languages of what that directive said.

Well, the Europeans adopted a directive on data protection that was effective in October of 1998. It applies to all of the EU member countries. For these purposes, the thing to underscore is that the Data Directive regards privacy of individuals as a fundamental human right. This bears out of some statements and some directives passed by the Organization for Economic and Cooperative Development and the [United Nations] in the early [19]80's, but privacy is expressly stated to be a fundamental human right.

Now, there are several states, numerous states, with state theories on privacy. There is a whole host of constitutional law in the United States, but no express statement, controlling statement, that from a policy perspective we want to regard privacy as a fundamental human right.

I may overstate that case with respect to the United States, but it is important to focus on this fact because it really portrays the difference in the way Europeans regard individual privacy and the way those of us in the U.S., particularly in the commercial sector in the U.S., regard privacy.

The Data Directive sets up an extensive regulatory structure. It requires that each country adopt what I will call for these purposes a data czar. And more than that, not just one data czar. There may be different enforcement mechanisms and regulators in different areas.

So, if you are a multi-national company that provides health care and financial information services, those may be governed

11. *See* James Harvey, *An Overview of the European Union's Personal Data Directive*, 15 No. 10 COMPUTER LAW. 19 (1998).

by two different data enforcement schemes in the UK [and] two different data enforcement schemes in Ireland. So for U.S. multi-national companies going to Europe, what this means is that, actually, instead of having one set of standard laws across Europe or one law, what you actually have is fifteen different implementations and then within each of those silos, you may have different subject matter areas that you have . . . to worry about. It exponentially increases the complexity and, indeed, the cost of companies moving to Europe.

The Data Directive also sets up a private cause of action. So not only can regulators come after those violating the Data Directive, individual citizens, Juan Fernandez in Spain, can come after American Airlines or Visa or anybody else for violations of the Spanish law.

Now, at this time I think there have only been nine of the fifteen countries that have actually adopted an implementing law implementing the Directive. The European Commission came out and really read the [riot act to] other countries that had not yet adopted a law, . . . saying, We are going to consider taking sanctions against you . . . if you don't adopt a law in compliance with the Data Directive.

But there is still this thing of, does a European citizen have a private cause of action even if there is no national implementing legislation? A very, very good theoretical question, but one that our clients are dealing with on a day-to-day basis.

What does the Data Directive require? It requires notice to individuals when you are collecting information from them and what type of information is being collected.

It requires choice. So, I give you this information in order for you to provide me with widgets via the Internet. If you would like to use that information for something other than providing me widgets, you have . . . to give me a choice as to whether you can do so.

Consent. I've got to give you my consent. Now, think about this in the online environment. How does one manifest assent? Is that via a click wrap, "I hereby agree," or do they have to sign something? It's something that Internet lawyers have been struggling with for a long time. But I will tell you that [when] most European counsel think of this consent thing, they kind of just hold onto the podium or hold onto their desk. They really want a handwritten signature waiving any privacy rights under these national implementing laws.

Onward transfer protection. So I'm selling you widgets via the Internet but I have a third party that actually does my billing services. They are not part of my company. They just do this on an out-source basis.

Well, the European Data Directive clearly requires that when you transfer that information to a third party, you have . . . to require the same protections that you afford to the individuals; you have . . . to require those protections from the third party.

. . . .

Access. This is another particularly thorny issue, particularly for United States companies. The European Data Directive says that you have to provide access to individuals with respect to all of the data that you have collected about them.

So if you have been in the widget selling business or the widget servicing business for twenty years, . . . [what] you have [is] these huge databases built up with respect to your customers [and] with respect to your products, . . . without regard to the reasonableness, the time frame in which the information was provided, [or] the cost that it will take to provide someone with access to their information. So, again, our friend, Juan Gonzales in Spain, if he goes to MasterCard and says, "Show me all of the personal data that you have collected about me," that is a very, very hard question for MasterCard to answer.

Adequacy provision . . . . What the Data Directive says is that no entity inside the European Union can transfer data to a country that does not have laws that are "adequate" to protect the privacy of European citizens. That is a very, very powerful provision, because essentially what they are doing is exporting their law to the rest of the world. And in the online environment, . . . borders are, if not superfluous, somewhat confusing.

There is one thing that is clear about privacy in the United States, and that's that the Europeans don't think that we have laws that are adequate to protect the privacy of European citizens.

Will it lead to a U.S./EU breakdown or prohibition of the transfer of data? I don't think so. When you think about that, the damage to the respective economies would be [too] large. But what's going on right now is an extremely uneasy truce between the U.S. Department of Commerce and the EU, and

then you have . . . the complicating factor of these fifteen implementing nations.

It has the effect of exporting the EU provisions around the world. So it's not just a U.S.-centric issue. If you are in Australia, if you are in Canada, Singapore, et cetera, you are worried: Are the Europeans going to say that data can't flow from Europe to my country? So you are starting to see a number of these jurisdictions around the world adopt or at least consider privacy legislation which is very much like the European Data Directive.

The last thing, in the U.S. we said, okay, let's create a safe harbor. Let's negotiate with the Europeans and create a safe harbor for U.S. web sites, such that if a site in the United States complied with the safe harbor, they would be free of enforcement actions from the European regulators, from the national data czars, as I've called them.

What does that safe harbor require? You will see a lot of the same elements: Notice, choice, consent, limited access rights, and self-enforcement. The status of this safe harbor is, it was supposed to have been adopted in October of 1998, roughly at the same time that the Data Directive was effective. Then it was mid winter of [19]99, then it was spring of [19]99. Then there was supposed to be a Clinton/EU Commission coming-out party in June of [19]99. That didn't happen. They can't agree, largely based on three issues . . . .

Limited access rights. The U.S. version of the safe harbor says that we will provide access to individual data when requested subject to, essentially, reasonableness constraints: How much it would cost us [and] whether it's really relevant.

So if Juan Gonzales goes to MasterCard just for a whim and says, Let me see all of my personal information, MasterCard would get to determine whether that was really relevant to Juan Gonzales or whether he had a legitimate beef with MasterCard or another party.

And, the cost factor. How much would it cost MasterCard to get Juan's information for him? That is at fundamental loggerhead with the European Union Data Directive and with the view of privacy in Europe.

Self-enforcement. As I said at the top of my comments, under the EU Data Directive they have set up elaborate regulatory schemes. Well, the U.S. and certain other countries around the world are not in favor of these regulatory schemes and they are saying, and in the safe harbor it says, you will self-

enforce. The FTC will step in, the state attorney general will step in, but you will subject yourself to audit by an independent third party, but it does not have any provisions in it for governmental oversight in a formal, regulated fashion as does the Data Directive.

I, quite frankly, don't know how—if they reconcile these things, it will be the greatest political compromise that I can remember.

Challenges. What are the challenges? Eighty-seven percent of net users are concerned about their online privacy pursuant to a—this is from a 1999 AT&T survey.[12]

I judge everything on the Internet by my mother. She's on her third computer now. She's very active on the computer. She does a lot of genealogy research, et cetera. I help her with her finances. She [uses] Quicken. She will not create a Quicken file and send it to me on the Internet because she uses Mindspring as an Internet Service Provider. She is scared to death that Mindspring is going to know how much money she has. She copies it onto a disk, puts it in a First Class mail envelope and sends it to me. She will not believe me—[her] son, the big city lawyer, all that kind of stuff—she just will not believe me when I say that is less secure than sending it to me over the Internet.

This is a very, very concerning thing. If E-commerce is going to change the world like many people think it will, if eighty-seven percent of net users are concerned about their online privacy, this is an issue that's going to have to be struggled with.

According to a Georgetown . . . privacy policy survey,[13] 361 "dot com" web sites were surveyed. Ninety-two point eight percent collected at least one type of personal identifying information.[14]

If you are out there on the net, your click stream data is leaving [and is] personal[ly] identifying. That means something that could either be used to identify or contact you. That's a stunning statistic.

---

12. *See* Lorrie Faith Cranor, Joseph Reagle, and Mark S. Ackerman, *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy*, AT&T Labs-Research Technical Report TR 99.4.3, (April 14, 1999). Available at <http://www.research.att.com/projects/privacystudy/>.

13. *See* Mary J. Culnan, *Georgetown Internet Privacy Policy Study*, (July 21, 1999). Available at <http://www.msb.georgetown.edu/faculty/culnanm/gippshome.html>.

14. *See id.*

Fifty-six point eight percent collected at least one type of demographic information.[15] So, did you come to their site from the east of the Mississippi or west of the Mississippi?

Sixty-five point nine percent posted some type of privacy policy.[16] I basically pay my light bill and my mortgage by advising companies about privacy and Internet issues, and I will tell you that I've read a lot of these privacy policies and I would not be misled by the sixty-five percent statistic. A number—all that it is, is a yes [or] no. Do they have a policy or not? That does not go into, is the policy effective; is it thorough; is it plain; can an end user read it and understand what's being said there? And it clearly doesn't go into . . . [whether] that company [is] following what they said they would do in the privacy policy. So don't be misled by that.

Individual challenges. Treat the schizophrenia . . . . I love My Yahoo.[17] I have it. I have a subscription to . . . the Interactive Wall Street Journal,[18] but I have this free thing from My Yahoo. I can follow sports. I could follow the volleyball team from the University of Montana if I so desired. It is absolutely great.

And . . . when I go to Amazon.com, they say, Welcome, James A. Harvey. Last time you were here, you bought a book on whatever, trout fishing . . . . I love that. But, on the other hand, Amazon, the other day, sent me an e-mail and said, You recently bought a book on, for example, trout fishing and we have . . . another series on X, Y, Z related to trout fishing. That was the most invasive thing to me. I found that to be very, very concerning.

I'm one of these schizophrenic net users. We have . . . to treat the schizophrenia. People need to decide on an individual day-to-day basis whether they like having the proactive e-mails or whether they would rather operate in anonymity.

Avoid state legislation . . . . What I do for a living is advise companies on Internet transactions. The more legislation that goes on, on a state-by-state basis, the harder it gets to do Internet and E-commerce in the United States.

And, when you think about it, it's almost a self-defeating endeavor because if Missouri passes a law, somebody is just

15. *See id.*
16. *See id.*
17. <http://my.yahoo.com/>.
18. <http://interactive.wsj.com/home.html>.

going to move to Arkansas. And if they move from Arkansas to Nevada, or whatever happens to be the appropriate jurisdiction, once they do all that, then they are going to go to Belize or Costa Rico or the Bahamas or any of a number of Internet havens, what I'm starting to call Internet havens, to get away from this type of legislation.

There may need to be federal privacy legislation and we can debate the pros and cons of that, but state legislation on privacy I think will be a step backward in terms of E-commerce.

Empower yourself. Behavioral solutions. Don't tell them how much money you make. Don't tell them where you live. Don't fill out surveys, et cetera. It's up to you to control your information. Read their privacy policies. See if they have a trust mark from TRUSTe[19] or Better Business Bureau Online[20] or from someone else, something that will let you know that a third party is looking at what they are doing.

Technological solutions. Anonymizer.com.[21] This is a site where they have essentially set up a technical solution that you can go there, get an alter ego for purposes of the Internet and, hopefully, travel around the Internet in relatively anonymous fashion.

It's subject to some debate whether they are successful at doing this. But, for example, on legal news groups, in order not to disclose who I am and to establish a client-attorney relationship with people, sometimes I use my anonymizer name to participate in those news groups so I don't leave a trail.

Passport[22] from Microsoft and digitalme.[23] These are technological solutions where Microsoft is saying, okay, give us all of your personal information, who you are, where you live, how much money you make, what your credit card number is, what kind of computer you are using, what you are interested in, your favorite sites and all that other good stuff. It doesn't exactly give me a warm and fuzzy to give that to Microsoft.

What Microsoft is saying is that when you go to Yahoo, you will use your Microsoft Passport and dole out your personal information to Yahoo . . . in a controlled fashion, so you know that your information isn't floating all around the Internet. Novell, with the digitalme, is another solution in this arena.

---

19. <http://www.truste.org/>.
20. <http://www.bbbonline.com/>.
21. <http://www.anonymizer.com>.
22. <http://www.passport.com>.
23. <http://www.digitalme.com>.

Again, I hope I don't offend anyone's sensibilities. In many ways, I regard Microsoft as like Darth Vader in Seattle. I really would not participate in Passport. I'm advising clients—clients generally come to me and ask, What can I do? And then I also encourage them to ask, What should I do? And Passport may be a tremendously valuable thing if Microsoft has their way, but I don't trust them and, quite frankly, I don't think most of the people in this room would trust them either. So, be ready for that.

What are the business challenges? Businesses have to create trust. In order for me to trust Amazon when they sent me what I considered to be an intrusive e-mail, they gave me the opportunity to e-mail them back and say, I don't want to participate in this, and they took me off the list. I haven't gotten any more e-mails like that, so they are creating trust with me.

MR. RENZ: Maybe I'm getting [ahead], but that's a question I have at this moment; and that is, at this stage of the game there is an economic incentive to ensure a customer's privacy. That is, if you come to me . . . and you buy my goods, I promise I will not pass this information on to someone else who will then e-mail you and so on.

I think the incentive is that in order to bring people into E-commerce who would not normally come into E-commerce because of the lack of trust—

MR. HARVEY: My mother.

MR. RENZ: Like your mother. But as E-commerce progresses ten and twenty years down the line, . . . I suspect it will be taken for granted, and the economic incentive and the fear of the anecdotal snowball effect that, Oh, I shouldn't get on the Internet because all of my privacy interests will be violated, as we get down and it's taken for granted, I suspect that incentive will be gone.

MR. HARVEY: I have a couple comments on that. One, I think there is, right now, a long-run economic incentive; and this is just an anecdotal observation based on my day-to-day practice. There is a long-run economic incentive to create trust.

The other incentive to create trust is to avoid state and federal legislation. Because if the legislators get in there and pass a law—I've been basically representing technology

companies for twelve years [and] every law that I've ever seen written that pegs to a certain technology has ultimately ended up being a failure because the technology changes. It's very difficult to write.

You know, the Constitution is one of the few things that endures well in the legal arena over time. And I don't think that writing a law based on today's Internet, what about DH—DHTML, XML, Internet 2, the next stage of the Internet? I'm worried about laws. But, today, I think that most companies are engaging in E-commerce without regard to privacy.

The large companies, the Yahoo, Amazon, et cetera, . . . are saying, Yes, it is in our economic best interest in the long run to behave in a proper, responsible fashion with respect to individual privacy.

The "also rans," the mid tier companies, when they come to me and ask for advice and I say, "What about Better Business Bureau; what about TRUSTe?" They say, "Is there a legal requirement?" And I say, "No, not in the United States." And for many of them, that ends the conversation.

So I think where we are right now is midstream, and as netizens of the world get more up to date, get more proactive, get more, quite frankly, more European like with respect to the privacy issue, you will see that economic incentive move from a future to a present. And I think you will see an avalanche of people coming out and saying, I will behave in a more responsible fashion.

Truste.org. This is a third-party enforcement program that was mentioned at the top of the comments, and Better Business Bureau. What they are trying to do is create a Good Housekeeping Seal of Approval. I tried to explain it to my mom and she said, You mean it's the like the tag that hangs off the end of the extension cord. And that's exactly it. When you see this tag, you know it's been approved.

So you will find these little trust marks on sites, and what they basically say is we have adopted a privacy policy that complies with these standards and we've agreed to let these organizations audit our practices with respect to our privacy policy.

. . . .

I think it was last week the FTC said [it] will start investigative actions when [it] receives complaints or notice from the third-party entities that a company has violated their privacy policy.

So this is the combining of the public and private entities out there in a way that the Europeans just don't think is sufficient.

. . . .

Avoid bloopers. I think it was 20-20, about four weeks ago, was accepting—they had some topic about some government agency and they were accepting e-mail questions, and they were also tracking the IP, the Internet address, of the servers that were generating those e-mails.

So someone sent in—you know, John from Bethesda sends in some comment or some question on this government-related issue. They track his IP address and they say, Wait a minute, the computer that John is originating from is from the federal department of so and so, . . . which completely undermined John's stance and it was—this was the manifestation of the privacy problem on television, and it created a big furor. Those types of things stick in people's minds.

Remember in the last nine months, . . . it came out that every Microsoft Word document that was created could be traced back to the computer on which that copy of Word resided, because they gave the registration information, et cetera. That is a big blooper that continues to scare my mom. She's still sending me Quicken files via First Class mail.

Legacy systems. For me, this is something that I deal with every day. I deal with large companies that are trying to move, A, to the Internet and, B, move their E-commerce efforts international.

What they have . . . is ten, fifteen, twenty years of databases built up of personal information. They don't know what information they have. They don't know how it's even being used. I've got 400,000 people in my company and I don't know what the Belgian division is doing with respect to the information in their databases on Belgian individuals.

And it's a huge expensive process. Taken to its logical conclusion it can make Y2K look like a minor blip on the computer radar screen. But it won't be taken to its logical conclusion because they will ultimately work it out in a more reasonable fashion.

Commercial negotiations. As big company A negotiates with big company B, three years ago who owned the data with respect to that relationship was not an issue. Now, it's a two-day protracted battle in certain circumstances as to who owns that data. As the law students in the audience get out and start

Montana Law Review, Vol. 61 [2000], Iss. 2, Art. 1

negotiating contracts on behalf of their clients, you will see this issue come up more and more. Who owns it? Who controls it? Whose privacy policy do we comply with in the course of this relationship?

Employee issues. There is nothing about the European Data Directive that's limited to just online endeavors. The Data Directive applies in the bricks and mortar world and in the electronic online world. So if you're big company A and you have . . . 100,000 employees in Europe [and] you are trying to ship all that information, cull that information, and send it back to the mother ship in the United States, that's a very difficult issue.

Adopt privacy policies. Again, economic best interest, whether it's short, intermediate or long-term; and I think it's what you ought to do and, hopefully, to avoid state and federal legislation.

Online and offline, the policies should address the common themes: Notice, choice, consent, opt in, opt out, access, and enforcement. Am I going to be a member of TRUSTe? Am I going to be a member of Better Business Bureau Online, or some other third-party enforcement agency that will let my mom know that a tag, in fact, hangs off the end of that extension cord and it's okay to use it?

That's, I think, my whirlwind tour of privacy on the Internet.