Buffalo Law Review

Volume 50 | Number 2 Article 4

4-1-2002

Colloquium on Privacy & Security

Gary M. Schober
Hodgson Russ

Shubha Ghosh
University at Buffalo School of Law

Ann Bartow
The University of South Carolina School of Law

Chris Hoofnagle
EPIC–Electronic Privacy Information Center

Phyllis Borzi
George Washington University School of Public Health and Health Services

TRANSCRIPT

Colloquium on Privacy & Security

GARY M. SCHOBER–MODERATOR
SHUBHA GHOSH–ORGANIZER
ANN BARTOW,
CHRIS HOOFNAGLE,
PHYLLIS BORZI–PANELISTS†

INTRODUCTION:

DR. BRUCE PITMAN, VICE PROVOST, SUNY BUFFALO

In the wake of a modern consumer there follows an electronic trail of e-tags, web cookies and database entries. Everyday transactions such as grocery purchases, movie rentals and health care visits are logged and stored. Businesses extol these data-collecting methods as promoting efficiency and productivity. Product and promotional decisions are made based on these data gathering and data mining activities, targeting, we are told, the right products to the consumer.

At a personal level, individuals worry that their medical records can be unfairly used in making employment or insurance decisions. Employee e-mail and web surfing are monitored by company IT professionals to protect company integrity. Meanwhile, advocacy groups decry the loss of privacy and the violation of self.

---

† This article is an edited transcript of the discussion held on Saturday, November 3, 2001 at the University at Buffalo as part of the Digital Frontier: The Buffalo Summit 2001.

Do we have a right of privacy that extends to aggressive tracking and record-keeping? Who guards the data and ensures its security? And who decides what uses of this data are legitimate?

On November 2-3, 2001, the University at Buffalo sponsored *Digital Frontier: The Buffalo Summit 2001*. The participants in the *Digital Frontier* were drawn from a wide range of specialties, from lawyers and doctors to businessmen and academics, in order to provide some perspective on our data-driven world. Speakers at the *Digital Frontier* addressed topics including Information Overload, Telemedicine, and Digital Artists.[1] A session on Privacy and Security identified some of the trends in technology that threaten privacy rights, as well as those that may assist preserving privacy. Speakers also explored legal developments and political structures influencing cyber-privacy. A transcript of the Privacy and Security session follows. We thank the speakers for their generosity both in speaking to us and in editing these transcripts. Thanks too to Dr. Jaylan Turkkan and her staff for organizing and, sometimes by sheer force of will, making the *Digital Frontier* an enjoyable and educating event.

TRANSCRIPT:

PRIVACY AND SECURITY IN AN INFORMATION AGE

SHUBHA GHOSH: The 2001 Digital Summit at the University at Buffalo has showcased a range of new technologies that will shape our future. In this panel, we focus on the question, what can we expect when this new technology is turned onto ourselves to pry into and collect information on the details of our lives? What happens to privacy and security as our technology grows in sophistication?

To help us in understanding these questions are four very distinguished lawyers. Moderating the panel is Mr. Gary M. Schober of Hodgson Russ in Buffalo. Gary will introduce the three speakers in detail, draw connections between their talks, add comments of his own, and facilitate questions and discussions. Gary is a partner at Hodgson

1. The Digital Frontier homepage is available at http://www.research.buffalo.edu/events/digital%20frontier/ (last visited May 16, 2002).

and is currently focusing his practice on issues of e-commerce.

Our first speaker will be Professor Ann Bartow of The University of South Carolina School of Law. She teaches Intellectual Property and Cyberspace Law, and she'll be speaking about the current legal treatment of privacy issues and the protection of privacy, especially private information held by businesses.

Our next speaker will be Mr. Chris Hoofnagle, who is Legislative Counsel at EPIC–Electronic Privacy Information Center in Washington, D.C. And he'll be giving us a comparative perspective of fair information practices in the U.S. and Europe.

Our last speaker will be Professor Phyllis Borzi, who is a research professor at the George Washington University School of Public Health and Health Services, and also a practitioner at the law firm of O'Donoghue and Donoghue in Washington, DC, where she does work in health law and ERISA. She'll be speaking about privacy in the healthcare area.

So let me just turn over the floor, then, to Gary who will give you some more comments.

GARY M. SCHOBER: Good morning, good to see everybody here on a Saturday morning. For those of you who are from Buffalo and keeping track, we are now 17 days away from the anniversary of last year's blizzard. So get ready. I did that for Ann's benefit. She came up from South Carolina and her first comment was, "I love the weather."

Ok, let's talk about privacy. I go around to all of my firm's regional offices giving a presentation on electronic commerce. Inevitably, no matter where we start, and whatever is going on in the world at the time, we end up spending most of our time speaking about privacy. People are very concerned about privacy. Businesses are concerned about privacy. And the government is concerned about privacy. Admittedly, some governments are more concerned than others, but nonetheless, there is real concern here. Why? Let me give you a couple of quick stories:

In my firm we have, as you would expect, access to the Internet. We also have an Internet policy, which by the way, we should all have. In that policy, the firm has the right to monitor usage of the Internet by its employees. And every now and then we look. We don't look very often–we all

have other things to do, thank God. But every now and then we do look. Most of the time what we find, we're a little embarrassed to say, is an occasional attorney looking at a pornography site, or something like that. We visit the offending lawyer, slap him around a little bit, and you rarely have it happen again. Usually the embarrassment factor is enough to dissuade people from violating the policy again.

One time we were monitoring Internet usage and, all of a sudden, I noticed that one of our young associates was looking at babies.com, strollers.com, and diapers.com, and I said, "Woops, guess what I now know?" We had a relatively young associate, on whom we were spending a lot of money trying to train her to be the very best lawyer she could be, checking out web sites relating to babies. I now knew she was pregnant! I didn't want to know, and she probably didn't want me to know, that she was pregnant, but I knew it.

Another quick story: we also have e-mail at the firm. Again, no big secret. And again, we have a policy on e-mail usage. Our e-mail usage policy says employees can use e-mail for reasonable, personal purposes. In drafting our policy, we compared e-mail to the telephone, and we don't pretend we're going to stop people from using it for reasonable, personal purposes. But every now and then, we have to go in and monitor usage–which again, our policy permits us to do. We usually monitor usage, as in the case of Internet usage, when there is a problem, if the system if going very slowly or there seems to be something wrong with what is going on. When that happens, it is typically caused by lawyers, not staff, trying to send pictures back and forth, that gobble up a lot of capacity. Well, one time we were monitoring to find out why the system was going very slowly, and I had to learn, not that I wanted to learn, that one of the staff members was having a homosexual relationship with another person who used to work at our office. I guarantee you, I did not want to know that. But while monitoring usage, I learned something that was very personal to one of our employees.

The problem is real. Those people should not have had to worry about what I was learning about them. At the same time, we're trying to run a business and we need to make sure that the tools provided to our people are used for legitimate business purposes. Like I said, we don't mind if

they send an occasional e-mail message wishing a friend happy birthday or something like that. But if we don't control usage of our e-mail system to some extent, the problem could get out of hand.

A related problem is security. Once I have all this information on my system, what obligation do I have to keep it secure? Today most of us rely on technical solutions for that. We have firewalls and other software products that we use. But what guarantee will my clients have, especially keeping in mind that I have a lot of confidential information on my system, that I will keep their information confidential and that the information will be secure from other people having access to our system?

The questions are obvious; the answers aren't so obvious. What are other countries doing? There has been a very different response to the issues of privacy. Some countries are moving much quicker than others. Some aren't moving at all. How does privacy fit in to the U.S.'s philosophy on self-regulation versus government regulation?

I think we've got a lot of interesting questions to talk about. I also think we've got three great speakers to talk about them. We're going to begin with Ann, who will give us an overview of the issues. Hopefully, she will elaborate on some of the topics I just raised. And then we'll turn to Chris and Phyllis, who will get a little more specific and focus the discussion, with Phyllis–interestingly–on medical information which obviously can be extremely sensitive. Forget about the information I've got on my firm's system–we lawyers think we've got lots of important stuff in our files and we obviously take a lot of pride in that–but imagine the sensitivity of information relating to one's medical history. Phyllis will help us discuss that topic.

We're going to begin right now with Ann, and we'll get moving. And then when we're all done, after all three speakers have gone, we'll open the floor to questions. I see we've even got microphones set out here, so we'll take your questions at the end. If you don't mind, hold them until then, and we'll address all of your questions as best as we can after the three speakers have gone. Thank you, and I turn it over to Ann now.

ANN BARTOW: Hi. One of the beginning debates in any discussion about the field of Cyberspace Law is always, is

cyberspace the same as real space, or is it different? Ultimately, the conclusion is always that in some ways it is the same, and in some ways different, but the debate in getting to that point is actually fairly useful when you consider some of the similarities and differences as a general matter. In the context of privacy, it is also a really good starting place, because in real space, customer data is collected and aggregated. Generally, in most transactions, there aren't a whole lot of representations made about data privacy, and little attention is paid to the fact that there are very few real space privacy policies anyway. In the absence of specifically targeted legislation, one example being the Video Privacy Protection Act;[2] or medical privacy, which one of our later panelists is going to talk about, the default rules of real space generally don't include any right to privacy.

So why is it, then, when we get to cyberspace we expect to have, or at least want to discuss, some right to privacy? Well, then we get into some of the differences between cyberspace and real space. In real space, when you buy groceries at the supermarket, you know the market is going to record what your purchases are. They may, in fact, record your credit card number. Maybe you have one of those "Smart Shopper" cards, so you get some discounts and they get to collect more information about you. But at the same time, they ordinarily don't stop and ask you for your age, your marital status, your educational level, or your family income before you attempt to buy your groceries. Nor does someone follow you around the store, making note of every product you inspect but then decline to purchase. The amount of data that is generated in cyberspace is a lot more substantial than the amount that is customarily generated in real space. And of course, the ease of collection is radically enhanced when they just have to follow your browser as opposed to following you around. The whole process is automated. However, as in real space, the common default rule is that there is no particular right to data privacy or informational privacy.

The justifications underpinning a right to privacy raise a lot of interesting questions. In general, the government has some constraints on its ability to collect and manipulate data about citizens. But any sort of restraint or constraint

2. Video Privacy Protection Act, 18 U.S.C. § 2710 (1994).

on private industry is only targeted specifically, as I said. Video rental records privacy came out of the Bork hearings, because when Judge Bork was nominated for the Supreme Court, his video rental records were released and published. And Congress went ahead and did this little patchwork legislation for video records, which probably saved Justice Thomas' bacon in his confirmation proceedings, because the press couldn't get his video rental records as a result of this Act. But in any event, there is a patchwork approach. I don't actually mean to characterize medical privacy as a little patchwork, because that is fairly substantial, but nevertheless, targeted privacy legislation, rather than any sort of over-arching principle, is what we see.

One of the questions that this raises for me is, why is it that we don't have any particular right to privacy in cyberspace or generally? But one of the questions that arises anytime people raise a right to privacy is, why do we need privacy? Why is it we are so afraid that people know our marital status, income or education level, or our religion? Not everyone who wants privacy is necessarily up to no good. That's always a suspicion, but in fact, there are a lot of good reasons why we like to keep information private. We maybe want to protect ourselves somewhat from identity theft, maybe we don't like being the victims, or at least objects of targeted marketing. And, as a general matter, whenever you have personal data compiled about you, people can make assumptions about you that you don't necessarily want them to make. Maybe they are incorrect, or as our Moderator said, maybe they are correct. Maybe the young associate he mentioned didn't want the firm to know that she was pregnant until later. This information got out. I would like to think our Moderator didn't treat her any differently, but I know as a woman who went through that experience of having a baby at a large law firm, that as soon as my pregnancy was known, I was treated differently. So, maybe this woman wanted to avoid that as long as possible, and she lost that option once the data compilation that had been done about her was known to her firm. She lost control over that information, which is a hard thing for everyone concerned.

There are other ways that this plays out that are sometimes sort of interesting. Data collection continues when one is responding to annoying or repugnant advertisement simply because the underlying product is of interest.

Here is something that happened to me recently: I am in the market for a new car. I did some research about cars on the Internet. I don't like a lot of the automobile advertising out there, and this means that ultimately I am probably going to buy a car from a company that runs ads that annoy me. When I was doing research on the cars, I looked at a company that I had purchased a car from before, and had been satisfied with. Like many lawyers, I am enough of a control freak that a manual transmission appeals to me. So I saw an advertisement touting a vehicle that featured a manual transmission. The car was of interest to me, but the advertisement was really irritating. Ultimately, I decided to click through so that I could find more information about the car. And I have to show you the tagline because you have to understand just exactly how irksome this was. The tagline for a car featuring manual transmission was, "Guys love girls who can drive a stick." That's really subtle, isn't it? So my question was, once I clicked on this ad–do I now go down in the cyber ledgers as some person who responds to this sort of sexist, idiotic advertising? And should I now expect more of it? And should I expect assumptions to be made about me because I was interested in that car, based on my response to this particular ad? I've also affirmed this sort of advertising philosophy, even though to my very core, I abhor the fact that I have done that.

The privacy policy on this particular automobile-related site wasn't too encouraging either. They were willing to give me lots of information about the car, but only if I provided my name, phone number, and e-mail address so they could contact me personally. And they noted they felt free to share my information with their partners. They did not specify who their partners were, or what they would do in terms of targeting a woman who would respond to an advertisement like this.

So that was sort of an odd exercise for me because I knew that they were going to make mistaken assumptions. I am generally not going to respond to advertisement like that on the whole, but there I was in cyberspace, looking like a person who would.

Personal information generally is valuable to a lot of entities, partly because it gives them the ability to do one-to-one marketing, and builds an electronic storefront that can be tailored to each individual. An online retailer could display products to suit a customer's perceived taste, their

price range, list customized specials–anyone who has surfed the Internet and shopped on the Internet has experienced this–and then the data in and of itself can actually be aggregated and sold or traded as a separate matter. On the one hand, they can use it to try to sell to you. But just collecting the data alone provides an asset that is valuable.[3]

Some of the techniques that are used generally involve following a person's click stream. When you go to the site, you click on banner adds or you click on certain links, you look at certain aspects of the website that are of interest to you, and your click stream can be followed page-by-page. However, this is not only when you're on one particular page, but they can then look at the pages that you move to afterwards. The click stream analysis can then be combined with collaborative filtering, and then observers can make educated inferences about your likes and dislikes, and compare your click steam analysis with your user profile. To the extent they can connect it to your real space behavior in terms of catalog shopping or other shopping habits, that might be done as well.[4]

Both passive and active information gathering occurs.[5] An active disclosure is generally voluntary. It is something you are aware you are doing: you fill out online registration forms and you answer surveys. You may, in return, get access to the site, as sometimes, active collection is required to gain access. Other times you may get rewards: sweepstakes entries, prizes, coupons or discounts for disclosing information. You are aware you are disclosing information, especially in that context. And I think at that point it feels like a *quid pro quo* exchange. The other time when it is active–but maybe doesn't feel quite as active–is when you disclose information in the context of a transaction. At that point, I think you feel you are giving the credit card number and your address because you want them to mail the product to you. I'm not sure it always registers with people that they are now voluntarily disclosing this information for any purpose. Nevertheless, it is characterized as an act of voluntary disclosure.

---

3. *See, e.g.*, Ann Bartow, *Our Data, Ourselves: Privacy, Propertization, and Gender*, 34 U.S.F. L. REV. 633, 647 (2000).

4. *See id.* at 654.

5. *See, e.g.*, Federal Trade Commission, *Self Regulation and Privacy Online: A Report to Congress*, (July 1999), *available at* http://www.ftc.gov/os/1999/9907/privacy99.pdf (last visited April 13, 2002).

And that contrasts with passive disclosures, the click stream monitoring that you are not aware of, that follows you around and collects your personal information, matching it up with other information available about you whenever possible. There is an awful lot of evidence out there that suggests that passively collected data is more accurate, and therefore it is more valuable. When people know that they are being watched and followed, they will self-censor. If they are not aware, their behavior is more true to their own characters and natures. Plus, when people are actively giving information, they will often lie. One reason they will lie sometimes is to have some privacy: so that outsiders don't know everything about them. To the extent information is passively collected about you, it is generally viewed as being more accurate and, therefore, more useful.

Most people are aware of one technique that is used to collect information, known colloquially as cookies or cookie files.[6] Cookie files are installed on a user's computer, and then they transmit information about how the user used the site. They welcome the user back to the website if the user goes back to the site on a later visit. A cookie file can record other sites that the user has visited, how the sited were used and then, sometimes, even information about the contents of the user's hard drive. Sometimes some sites or some computers will be set so that the user knows that cookies are being put on a user's hard drive, in that case it is almost appears to be permissive disclosure–you know that there is a cookie there–although you don't necessarily know what it is doing there or what it has collected. To the extent you permit your hard drive to accept cookies, you should then assume everything you do will be monitored. And, cookie files can also be installed without a user's knowledge, therefore leading to the unknowing passive disclosures that create more valuable data. Cookies are there but you wouldn't be aware of them.

Many sites will not allow you to access them, or at least most of the content in the site, unless you are willing to accept a cookie file. Cookie files are sometimes spun as being very useful to the user. And to some extent that is

6. For a brief explanation of "cookies," *see* http://www.privacyfoundation.org/resources/glossary.asp#Cookie (last visited May 16, 2002); *see also* Bartow, *supra* note 4, at 678-79.

true, although the reasoning here is very circular. One of the things that many sites will ask you to do is come up with a user name and password. And you would need a separate user name and password if you buy books at Amazon.com, buy toys at eToys, and buy diapers at Diapers.com–each individual site would ask for its own user name and password, which gets to be maddening over time, trying to keep track of them all. So to do you a favor, the cookie file will enable you to keep your registration handy, so you can log on without inputting your user name and password each time–it will also keep your address and phone number and e-mail address and your credit card number at the ready to make it as convenient as possible for you to shop. So it spins as an object of convenience, but my question is, why do you need the user name and password in the first place? It does make it easier if I don't have to remember the user name and password for Diapers.com because I don't have a baby and don't buy them very often. I wouldn't be visiting the site very often and trying to keep track of my Diapers.com user name and password without a cookie file would be a hardship. But why I need the password to get there in the first place confuses me, and it is really not about my convenience so much as about their slippery slope argument that the easier it is for me to buy with one click, or the fewest clicks and least amount of inputing and effort, the more buying I do. If I actually have to get my credit card out of my purse and re-enter the number, I might have buyer's hesitation and decide not to purchase things after all. So it is really not about my convenience, so much, as it is about selling me as many goods and services as possible.

Another technique for gathering data that has emerged involves web bugs, which are tiny, often transparently embedded in the graphics on web pages.[7] They can report an IP address and cookie information. They can work with cookies, referring a URL to the site's owner. Many e-mail clients read HTML mail, and to the extent you do that, web bugs can be passed along because they can be inserted in e-mail so that the person who sent the web bug can now follow your e-mail and see if you forward it or delete it –

7. For more information on "web bugs," see http://www.privacyfoundation.org/resources/webbug.asp (last visited May 16, 2002).

exactly what you do with the e-mail. In that way, targeted e-mail marketing can be assessed and monitored. It is also possible for them to match the e-mail address up with where it has gone, and personally identifiable information can be accessed with a previously set cookie. Unlike cookies, you are almost never warned that there is a web bug, and anti-cookie filters won't catch them. So they can do a whole lot better job of tracking surfers in areas without banner ads, or in other places where even reasonably savvy people wouldn't expect to be trailed.

Because so much data collection is going on, and because so much attention is being paid to this recently, one government agency that responded to some of the questions that came up involving privacy was the Federal Trade Commission (FTC). I know another panelist is going to speak in more detail about it, but one of the things the FTC has done is to recommend fair information practices involving notice, choice, access, and security. It was interesting that the FTC is the agency that sort of stepped up to bat, in terms of being a government agency that took over privacy. There is nothing particular about privacy that would suggest right away that privacy is the purview of the Federal Trade Commission. As part of its mandate, the FTC is supposes to observe commerce and it is supposed to look into unfair and deceptive trade practices. A professor at the Vanderbilt University School of Law, Steven Hetcher, has written a really interesting article called *The FTC As Privacy Norm Entrepreneur*.[8] One of the things he does in that article is chart how and when the FTC started asserting jurisdiction over privacy. And there is a lot going there.[9] On the one hand you can say the FTC legitimately has an interest in privacy, but the agency also seems to have an interest in expanding its own power, jurisdiction

8. Steven A, Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041 (2000); *see also* Steven A. Hetcher, *The De Facto Federal Privacy Commission*, 19 J. MARSHALL J. COMPUTER & INFO. L. 109 (2000).

9. *Hetcher, The FTC as Internet Privacy Norm Enterpreneur, supra* note *8,* at 2061 ("Pursuant to the Federal Trade Commission Act, the FTC regulates unfair and deceptive trade practices. Unfairness, per se, is too uncertain of a standard to seek enforcement actions against websites that take data without notice or consent, however. But once websites are induced to make representations in writing via privacy policies, then it is easier for the FTC to seek enforcement actions for deceptive trade practices. Thus, the public choice explanation of the Agency's promotion of privacy policies is that this activity allows the Agency to increase its jurisdiction.").

and funding, as any organization will tend to do. And one of the interesting developments is that web sites that voluntarily adopt but do not strictly follow privacy policies have really worked in the FTC's favor in this regard. A site that doesn't have a privacy policy, may have its business practices questioned, but not having a privacy policy only vaguely falls under the rubric of unfair. It is kind of nebulous and it was almost hard for the FTC to assert jurisdiction under the general idea that collecting information without notice is unfair. Once a web site has a privacy policy, if the company doesn't follow it, now suddenly they're squarely within the realm of deceptiveness. Instead of just being an unfair trade practice, that's a deceptive trade practice, which gives the FTC more leeway to assert jurisdiction, and the agency was only too happy to do that. Once web site privacy policies became more common, deception became a greater possibility, and this made it easier for the FTC to assert broad-based jurisdiction over privacy policies.

Web sites are not legally required to have privacy policies, nor are they required to follow the fair information practices recommended by the FTC. But when the FTC notes that a web site fails to comply with its own privacy policy, that is when the FTC will step in. This contrasts, interestingly to me, with Congress' approach to privacy. A lot of bills have failed to pass or are pending. I think about fifty at this point, but none of them is particularly likely to pass, nor is the government likely to take a more assertive role in requiring privacy policies or in requiring fair information practices any time soon. And one of the things that is fascinating to me, as a person who teaches cyberspace law and tries to follow the area, is the way privacy is treated differently from other spheres of the law. Dick Armey, a republican from Texas, is one of the people who has been a vocal opponent of privacy policies. When some of the pending privacy legislation was proposed, he sent a letter to his colleagues that said, and I quote, "Congress is an inexperienced and amateur mechanic trying to tinker with a supercharged, high-tech engine of our economy. We need to be careful not to let our good intentions get in the way of common sense."[10] So it was a

10. Dick Armey, Privacy: *For Those Who Live in Glass Houses*, (April 9, 2001) *available at* http://www.freedom.gov/library/technology/memo/privacy.asp

clear signal from him that Congress shouldn't tamper with the Internet, or shouldn't do any regulation of the Internet. And if that were their consistent approach, you might say, "Okay, they just want to take a laissez-faire view of the Internet." But, in fact, once you start looking at things like "decency" and pornography, they're only too happy to regulate. You look at the Communications Decency Act,[11] the Children's Online Protection Act,[12] the Children's Internet Protection Act[13]–when they're talking about sex they're only too happy to do content regulation. It is only when privacy is the issue that Armey says, "Oops, we shouldn't interfere with the Internet." But as for content regulation I could go off on copyrights regulation and other intellectual property regulation in addition to sex, and then Congress seems only too happy to get involved with the minutia of the Internet. Yet Dick Armey and other Congressional Representatives criticized the FTC for suggesting that regulating Internet privacy might be necessary.[14]

The Geocities case was the first case where the FTC flexed its privacy muscles. Geocities had made some promises in its privacy policy about not sharing data with third parties, and then it went ahead and shared it anyway.[15] And so the FTC got involved, filed a complaint, [16] and ultimately settled with Geocities.[17] And Geocities wound up agreeing to a regimen of privacy that was much stricter

---

(last visited April 14, 2002); *see also* John L. Micek, *U.S. Urged to Focus on Consumer Privacy*, E-COMMERCE TIMES, *available at* http://www.ecommercetimes.com/perl/story/8871.html (last visited April 14, 2002); Tech Law Journal Daily E-Mail Alert, no. 162, (April 10, 2001) *available at* http://www.techlawjournal.com/alert/2001/04/10.asp (last visited April 14, 2002).

11. Communications Decency Act, 47 U.S.C. 223 (1994 Sup. IV 1998) found unconstitutional by Reno v A.C.L.U., 521 U.S. 844 (1997)

12. Child Online Privacy Protection Act, 15 U.S.C. S. 650 (1998).

13. Children's Internet Protection Act, 20 U.S.C.S. 6301 (2002).

14. *See generally*, Armey, *supra* note 10.

15. *See* James Glave, *Feds Slam GeoCities on Privacy*, WIRED NEWS, *available at* http://www.wired.com/news/politics/0,1283,14412,00.html (last visited April 14, 2002).

16. The F.T.C.'s complaint can be viewed at http://www.ftc.gov/os/1998/9808/geo-cmpl.htm (last visited April 14, 2002).

17. Press Release, Federal Trade Commission, Internet Site Agrees to Settle F.T.C. Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case, (August 13, 1998) *available at* http://www.ftc.gov/opa/1998/9808/geocitie.htm (last visited April 14, 2002).

than anything that the law currently requires.[18] Geocities agreed, once the FTC intervened, to revise and upgrade their privacy practices. Geocities agreed to follow its privacy policy, and the new privacy policy was much stricter than anything it had agreed to before, and it actually even exceeded some of the mandates of the FTC's fair information practices. So that was interesting. Once the FTC got involved, you did see an upgrade in privacy–at least on the Geocities' sites–which I think sent a message that either other sites should not have a privacy policy and then they don't have to worry about it, or if they did have one, to follow it, because otherwise the FTC could possibly take action.

The Toysmart case came up in a little bit different context. Toysmart was a dot.com that was selling toys over the Internet. It was largely funded by the Walt Disney Company and, like so many dot coms, it didn't have a great business model and wound up hemorrhaging money fairly quickly. Once it was in bankruptcy–or at least in danger of bankruptcy–there weren't a whole lot of assets. One of the first things done was that an ad was run in The New York Times that said, "We will sell you our data. We will sell you the names and addresses and family profiles of everyone who is registered with our site." And that data looked to be about the biggest asset Toysmart had with which to pay creditors. The little problem, of course, was Toysmart had a privacy policy that said "we will not share your data with third parties." So a couple of players got involved. The FTC got involved;[19] the attorneys general of several states got involved and were interested in this.[20] And also TRUSTe,

18. Bureau of National Affairs, *Is GeoCities Consent Order the F.T.C.'s Privacy Regulation of Tomorrow?*, ELECTRONIC COMMERCE AND LAW REPORT (Sept. 2, 1992) *available at* http://www.perkinscoie.com/resource/ecomm/privbna.htm (last visited April 14, 2002).

19. Press Release, Federal Trade Commission, F.T.C. Sues Failed Website, Toysmart.com, for Deceptively Offering For Sale Personal Information of Website Visitors (July 10, 2000) *available at* http://www.ftc.gov/opa/2000/07/toysmart.htm (last vistited April 14, 2002).

20. Melanie Austria Farmer, *Toysmart Suspends Auction of Customer List*, (July 27, 2000) *available at* http://news.com.com/2100-1017-243718.html (last visited April 14, 2002); Linda Rosencrance, *Update: Attorney General Still Seek to Block Toysmart Data Sale*, (August 26, 2000) *available at* http://www.computerworld.com/cwi/story/0,1199,NAV47_STO47510,00.html (last visited April 14, 2002).

which I'm going to talk about in a second, which is a seal organization, also took note and complained about this.

After all those players got involved and started criticizing the sale of data, the bankruptcy lawyers and bankruptcy judges started wondering how they were going to handle all of this, because the rules of bankruptcy are very different than the rules of normal human society in terms of just trying to find assets and sell them at all costs.[21] They weren't worried about privacy, they wanted to maximize money for creditors and that conflicted fairly dramatically with any interest in privacy. If this data was the main asset, the bankruptcy folks were real eager that it be valued and sold. So that was a pretty interesting development. Ultimately the FTC decided that the data could be sold but only under certain conditions.[22] The bankruptcy judge begged to differ, however.[23] We didn't see any court actions spin out because the Walt Disney Company, which took a lot of criticism for this because they said they were a major investor in Toysmart, purchased the data for $50,000 and then destroyed it, and they did that mostly as a public relations issue.[24] So we didn't see the dispute spin out in court and get a chance to see what a non-bankruptcy judge thought the law in this area might be.

One of the few places that Congress has decided to act on Internet privacy involves children. The collection of data from children was also an issue in both the Geocities and Toysmart cases. Geocities presaged COPPA the Children's Online Privacy Protection Act.[25] Geocities was facilitating the collection of personal information from kids. They

21. Nicholas Morehead, *Toysmart: Bankruptcy Litmus Test*, WIRED NEWS (July 12, 2000) *available at* http://www.wired.com/news/business/0,1367,37517,00.html (last visited April 14, 2002).

22. Elizabeth Blakey, *After the Toysmart Debacle*, E-COMMERCE TIMES (July 25, 2000) *available at* http://www.ecommercetimes.com/perl/story/3868.html (last visited April 14, 2002).

23. Michael Brick, *Judge Overturns Deal on the Sale of Online Customer Database*, (August 18, 2000) N.Y. TIMES ON THE WEB *available at* http://www.nytimes.com/library/tech/00/08/biztech/articles/18toys.html (last visited April 14, 2002).

24. Gavin McCormick, *Judge Approves Toysmart Data Deal*, (Jan. 30, 2001) *available at* http://boston.internet.com/news/article/0,,2001_574121,00.html(last visited April 14, 2002).

25. 15 U.S.C. S. 650 (1998).

pretended like it was not them that was doing it, but they were actually letting third parties collect information about children. That didn't really smell right, apparently, to the FTC and was labeled deceptive.[26] Eventually Congress passed the Children's Online Privacy Protection Act, which does give some data privacy protection for children under 13. And then Toysmart came afterwards. One of the things that the FTC noticed, as it was looking into the Toysmart case, was that Toysmart was not complying with the Children's Online Privacy Protection Act.[27] They were collecting information from kids in violation of the requirements of the Children's Online Privacy Protection Act. In fact, there has been some anecdotal evidence that almost no one is complying with it and people are just trusting the fact that there is almost no enforcement, so they won't get caught.

One of the motivating factors for this legislation was actually pedophiles. It wasn't entirely about getting businesses to stop collecting information from kids. It was one more way to work against adults that were trying to meet kids on the Internet, although it certainly does apply to businesses. There are several uncertainties concerning the Act. There are some questions about what consent from parents is.[28] There are some rules that were issued by the FTC,[29] and there are also some loopholes. The one that

26. *GeoCities Settles with F.T.C. on Kids' Data Complaint*, (June 15, 1998), *available at* http://www.internetnews.com/IAR/article/0,,12_6921,00.html (last visited April 14, 2002): James Glave, *F.T.C. Spanks Kids Site on Privacy*, WIRED NEWS (May 6, 1999) *available at* http://www.wired.com/news/politics/0,1283,19542,00.html; Tim Wilson, *F.T.C. Reaches Privacy Settlement With GeoCities*, (August 14, 1998) *available at* http://www.internetweek.com/news/news081498-2.htm (last visited April 21, 2002).

27. Keith Perine, *Toysmart Settles With F.T.C.*, (July 21, 2000) *available at* http://www.thestandard.com/article/display/0,1151,17051,00.html (last visited April 21, 2002).

28. *See, e.g.*, Lynn Burke, *Contending With COPPA Confusion*, WIRED NEWS (August 23, 2000) *available at* http://www.wired.com/news/politics/0,1283,38332,00.html (last visited April 14, 2002).

29. *See* Press Release, Federal Trade Commission, New Rule Will Protect Privacy of Children online (October 20, 1999) *available at* http://www.ftc.gov/opa/1999/9910/childfinal.htm (last visited April 21, 2002); *See also*, Federal Trade Commission Facts for Businesses - *How to Comply With the Children's Online Privacy Protection Rule* (November 1999) *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm (last visited April 21, 2002); Margret Johnston, *F.T.C. Issues Rules on Child Privacy Act*, IDG NEWS

troubles me the most as a parent is that schools are allowed to make decisions for the kids about data, and they don't need the parent's consent: they can act as the parent.[30] So, schools that are desperate for money are selling candy in the schools and selling companies the ability to put their logos in the schools are not really institutions I trust not to sell my kid's data to businesses that want to purchase it from the schools. I think that is a pretty significant loophole and also very worrisome.[31]

As our moderator already mentioned, there is also a data privacy culture clash with Europe. One of the issues is that many European countries, for cultural reasons, are much more protective of personal information privacy. And one outcome of that has been the European Data Privacy Protection Directive that was adopted, and became something that e-commerce people in the United States had to deal with.[32] Ultimately, a "Safe Harbor" agreement was negotiated.[33] The requirements for Safe Harbor under the Directive are notice, choice, onward transfer access, and security data integrity enforcement issues.[34] Again, I'm happy to provide you with more specific information, outside of this speech about all the requirements of the Directive, but ultimately, to the extent that U.S. companies comply with this, what it winds up doing is giving Europeans a whole lot more privacy than we Americans have. The e-commerce entities only have to comply with these requirements with respect to Europeans, so when Europeans do e-commerce with U.S. sites, they get privacy protection. When United States citizens do e-commerce with the same sites, we don't get those protections. American children get less privacy online with COPPA than European adults do under the Directive.

Several market-based "solutions" have been proposed–

SERVICE (October 20, 1999) *available at* http://www.idg.net/idgns/1999/10/20/UPDATEFTCIssuesRulesOnChild.shtml (last visited April 21, 2002).

30. *See* Press Release, *supra* note 30.

31. *See, e.g.*, Bartow, *supra* note 3, at 658-62.

32. *See id.* at 662-64.

33. For more information on the "Safe Harbor" agreement, see http://www.exports.gov/safeharbor/ (last visited April 14, 2002).

34. For a list of organizations tha have notified the U.S. Dept. of Commerce of their adherence to the Safe Harbor framework, see http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list (last visited April 14, 2002).

and I have the word solutions in quotes–to the privacy issues I've raised, including opt-in and opt-out data collection, ad-blocking software, and other issues and then the seal issue which I want to finish up with. Opt-in data collection is the idea that you only collect data from people that agree that you can do that, who "opt-in", and then data collection presumably can be a fairly active process, and a knowing process.[35] But, as I said before, knowing that you are being observed devalues the data. If people know they're being followed, their clickstreams and personal information are not as valuable.[36]

Opt-out data collection–the idea that data is going to be collected from you unless you say, "stop it"–has some potential, except that when you opt-out of the data collection, generally you opt out of accessing the site.[37] For example, consider The New York Times site: if you will not sign in and disgorge personal information, then you just can't read the paper online. So when you opt out of the collection you just kind of opt out of that part of cyberspace, which I find fairly troubling for a lot of reasons.

Ad-blocking software offers some promise as well. If you don't get the banner ads, you're not tempted to click on them and they can't follow your click stream. But in fact, many e-commerce sites will simply not allow you to access them. They can figure out that you are using ad-blocking software, and if you're not going to play by their rules, and view their ads, you're not going to access their site.[38] The same with cookie crumbling and web bug fumigation: There may be technological fixes, but again, to the extent you use them and the sites figure out you're using them, they will generally deny you access.

The next private industry solution that government, and for a while the FTC was even touting, involved trusted seals. The idea being that certain seal organizations similar in some ways to the Good Housekeeping seal of approval would set up a framework of privacy and then every site would have to agree to comply with that framework, and then it could bare the seal. And the idea being when you went to a site you would look for a seal. And if you saw the seal there you could be assured that at least minimal

35. *See* Bartow, *supra* note 3, at 683.
36. *Id.*
37. See *id.* at 681.
38. See *id.* at 677-78.

privacy guarantees would be in place. The two largest seal organizations are TRUSTe[39] and BBB Online, which is the Better Business Bureau Online.[40] However, how this plays out is not exactly reassuring.[41] The New York Times Privacy Policy says, in part, "[t]his overall privacy statement verifies that the New York Times on the Web is a member of the TRUSTe program and is in compliance with TRUSTe privacy principles. We also participate in the Council of Better Business Bureaus' BBB Online Privacy Program and comply with all BBB Online Privacy standards."[42] So it asserts–The New York Times asserts–that its privacy policies follow and comply with both seal programs. When you look at what the seal programs require, TRUSTe says you'll be notified of what personal identifiable information is being collected, when it is being collected, how it will be used, how it will be shared, what choices are available to you, what use and distribution will be made, and what kind of security procedures are in place[43]–which sounds pretty good. It sounds pretty darn reassuring. BBB Online is similarly reassuring. It says, "BBBOnLine's mission is to promote trust and confidence on the Internet. . .[and] BBBOnLine Privacy awards seals to online businesses that have been verified to be following good information practices."[44] Notice they say "good information practices" but not fair information practices, because neither regimen rises to the level of the FTC's fair information practices. And in fact, you look at what TRUSTe requires, you look at what BBB Online requires, and you are fairly assured until you consider the fact that The New York Times asserts that it complies with both of them, and then you read in full The

39. TRUSTe's homepage is available at http://www.truste.org/ (last visited April 14, 2002).

40. BBB Online's homepage is available at http://www.bbbonline.org/ (last visited April 14, 2002).

41. *See* Bartow, *supra* note 3, at 669.

42. N.Y. Times Customer Service Privacy Information is available at http://www.nytimes.com/ref/membercenter/help/privacy.html (last visited April 14, 2002).

43. The N.Y. Times Customer Service Privacy Information also provides a section regarding TRUSTe, *available at* http://www.nytimes.com/ref/membercenter/help/privacy.html#truste (last visited April 14, 2002).

44. The N.Y. Times Customer Service Privacy Information also provides a section regarding the BBB Online, *available at* http://www.nytimes.com/ref/membercenter/help/privacy.html#bbb (last visited April 14, 2002).

New York Times Privacy Policy. And what you find is that The New York Times Privacy Policy requires you to permit collection of personally identifiable data, which is both actively and passively collected. It requires acceptance of cookie files from The New York Times and from third party advertising companies using The New York Times site. It permits The New York Times to log IP addresses and it permits The New York Times to share the information it gathers with "advertisers and other partners." The New York Times doesn't tell you what information will be given to these partners, and it doesn't even tell you who these partners are. So why is it that this policy complies with TRUSTe and BBB Online? I think it is because the requirements are so incredibly weak. If the New York Times' so-called privacy policy, with these elements, complies with the mandates of those seal programs, I don't think the seal programs are really all that useful in protecting privacy–at least not as I envision privacy.

What conclusions do we draw? First, privacy policies are optional. Second, they can be very, very weak–yet still appear meaningful because they can bear these seals and look like they participate in consequential seal programs. One thing that companies need to be aware of, though, is that if they are going to have privacy policies, they must at least comply with their own policies. And once you voluntarily adopt a privacy policy, you are bound by it–at least according to the FTC–although there is some fuzziness in their jurisdiction and about what ultimately they can do to enforce voluntary privacy policies. A privacy policy however, is not an inherently binding document unless the terms of the privacy policy says that it is. And in fact, most privacy policies are quite mutable–often explicitly so. There will inevitably be a term in the policy that says, "We reserve the right to change this privacy policy at our discretion." And in fact, they can be changed to adapt to the shifting legal terrain of data privacy. After the Toysmart case got attention, large e-commerce sites like Ebay and Amazon.com started sending notices to their members, basically saying we're changing our privacy policy now, just so you know, and if we're ever in bankruptcy we're selling your data.[45] So they just changed

45. *See, e.g.*, Keith Regan, *eBay Modifies Privacy Policy With Toysmart in Mind*, E-COMMERCE TIMES (April 3, 2001) *available at*

their privacy policies. At some point I would hope that contract law principles would be applied to privacy policies so they couldn't be unilaterally changed like that, and would be binding on both sides. But that is not the case at present. There is no case law that suggests it has happened yet, and there are no trends that suggest it will happen any time soon.

So thank you for allowing me to give you this overview of privacy–or lack thereof–in cyberspace. And, at the end, I look forward to any questions

GARY M. SCHOBER: Thank you, Ann. Please keep in mind as we go through this–because Ann and I really did the same thing–we are focusing on businesses collecting information, usually in the context of the Internet, doing business online, or something similar to that. Don't forget, there are others out there collecting information as well, the government being probably the biggest example. Both the government and private businesses also collect information in a non-internet context. I go online and I want to buy a book from Amazon.com. There is a little bit of activity on my part. I am consenting to and participating in the transaction. However, as electronics become more sophisticated and more a part of our lives, there isn't always that option. My favorite example is something most of us in New York use these days, the EZ-Passes. A number of other states also have it, although not all. But EZ-Pass has enabled us to go through our tollbooths very quickly. Downstate it is a little bit different than it is up here. If you drive much down in the New York City metropolitan area, you quickly realize that they have structured the tolls so that you almost have to get an EZ-Pass. Because there is only going to be one or two lanes that will take cash, and the rest of them take the EZ-Pass, if you have ever tried to cross the George Washington Bridge, you know that getting in one of those

---

http://www.ecommercetimes.com/perl/story/8654.html (last visited April 14, 2002); Jeffrey Benner, *eBay alters Privacy Policy*, WIRED NEWS (April 2, 2001) *available at* http://www.wired.com/news/business/0,1367,42778,00.html (last visited April 14, 2002); Keith Regan, *Amazon Announces Controversial Privacy Policy*, WIRED NEWS (April 2, 2001) *available at* http://news.com.com/2100-1017-245676.html?legacy=cnet (last visited April 14, 2002); Associated Press, *Privacy Groups Break Ties With Amazon*, (Washington, Septmber 14, 2000) *available at* http://www.ecommercetimes.com/perl/story/4180.html (last visited April 14, 2002).

two lines that only accepts cash is not something you want to do. So you are forced to get an EZ-Pass, if you're going to be driving down there with any frequency. Well, let me tell you a recent story that happened to me. I have a habit of going through the EZ-Pass lanes–we don't have any policemen here, do we–a little too quickly. One day I get a letter, and it was brutal. "Dear Slime Bucket, you went through the EZ-Pass lane at 25 miles an hour. Don't you know you're only supposed to do it at 5? If you ever do it again, we're going to take your EZ-Pass away, we're going to take your car away, we're going to take your kids–well they can have the kids–we'll take everything you've got." I said wow and then started thinking about it. Forget about my going through the tollbooth too quickly. Think about my trip from Buffalo to Rochester. They know what time I go through the Buffalo tollbooth, and they know what time I go through the Rochester tollbooth. You don't need to be Einstein to do the arithmetic here. They know what my average speed was all the way down the thruway–and if you watch Law and Order, you know they'll get me one of these days. I expect to receive my ticket via first class mail. Anyway, I just wanted to make sure we keep in mind that there are more subtle privacy issues lurking behind the scenes.

To keep us going, we're now going to turn things over to Chris, who will talk about privacy and some of the things perhaps that the FTC has been up to–or as Chris would put it, some of the things they haven't been up to.

CHRIS HOOFNAGLE: Thanks so much for having me today. It is a pleasure to come out to Buffalo and to come to this fine facility and talk about an issue of heightened public concern, especially after the September 11 attacks. It is either a Chinese proverb or a Chinese curse when one says "may you live in interesting times." We are certainly living in interesting times now. I think one of the challenges that we face as we go forward in life is recognizing the new revolutions, the new issues that will define our culture and will define our generation. And one of those issues is privacy. We at the Electronic Privacy Information Center think that privacy is the civil rights issue of our generation–that people who grow up after my generation, after your generation will have heightened expectations of privacy. They will have heightened protections in law–we

hope as well. We are seeking baseline legal protections that are complemented by privacy-enhancing technologies in order to put individuals in control of their personal information.

So consistent with that, let me tell you a little bit about EPIC and then go into Fair Information Practices (FIPs). I also will summarize commercial and governmental threats to privacy that exist that may not be apparent to most individuals. I second everything Professor Bartow said today. She is making my job really easy here–I can really delve into the deep matter I wanted to talk about today based on her excellent presentation. EPIC is a public interest non-profit group in Washington, D.C. We maintain a website at www.epic.org, where we have an archive on privacy issues. We also run a news site at www.privacy.org. I welcome you to visit it. We also sell a number of books relating to privacy, the First Amendment, and Human Rights. The gold standard in privacy is the idea of FIPs. FIPs recognize that entities, whether they be government or commercial, assume certain responsibilities when collecting personal information. FIPs can address the risk and responsibilities that collection of personal information entails. It is interesting, FIPs were born in the United States. However, notions of privacy exist in the oldest texts known to mankind. There is recognition of privacy in the Qur'an,[46] the sayings of Mohammed,[47] and in the Old Testament.[48] But the idea of Fair Information Practices originated in the United States during the 70's. The Health Education and Welfare Committee on Automated Personal Data Systems–noting the potential of computers to collect information on individuals–developed the idea of Fair Information Practices. Health Education and Welfare recommended that FIPs in fact be codified. They thought there should be an individual right of action so that if FIPs were violated, someone could walk into their local court-room and sue the government.

What happened as a result was the Privacy Act of 1974

---

46. an-Noor 24:27-28 (Yusufali); al-Hujraat 49:11-12 (Yusufali).

47. Volume 1, Book 10, Number 509 (Sahih Bukhari); Book 020, Number 4727 (Sahih Muslim); Book 31, Number 4003 (Sunan Abu Dawud).

48. RICHARD HIXSON, PRIVACY IN A PUBLIC SOCIETY: HUMAN RIGHTS IN CONFLICT, 3 (Oxford Univ. Press 1987). *See* BARRINGTON MOORE, PRIVACY: STUDIES IN SOCIAL AND CULTURAL HISTORY (1984); *see also* JEFFREY ROSEN, THE UNWANTED GAZE (Random House, 2000).

and a secondary Privacy Commission that studied these issues.[49] And they went even further. The Second Privacy Commission said that we should not only codify FIPs, we should codify them so they apply against private business as well. That never really took hold, and we have a schism in American law where the Privacy Act of 1974 that has great protections–although many of them have been watered down–for citizens against government collection of information. But the private sector really has free reign. And since corporations have individual rights–corporations had individual rights before women did, which is a very sad comment on our Supreme Court–these corporations operate with their own rights to privacy, including copyright and trade secrets.[50] And so many of the commercial practices that I am going to highlight today are not transparent to users but if the government perpetrated them, we would have substantative rights in law to control these practices. Individuals are not aware of private-sector abuses of privacy, and cannot discover them unless they are exposed in litigation or in newspapers.

With that said, let me talk about some Fair Information Practices. The FTC recognizes four FIPs: notice, choice, access and security. The Organization for Economic Cooperation and Development (OECD), went much further in 1980. And many EU member states now have privacy directives that that codify a general right to privacy against government and commercial sector invasions of privacy in the framework of FIPs. The most important protection in this area is the idea of "minimization:" one should not even transmit personal data unless it is necessary. We should minimize the exposure of personal data by only transmitting the minimum necessary to complete a transaction. The commercial world follows the exact opposite. There are a number of consultants who say that commercial entities should collect as much information as possible. When you sell someone a television, ask them what their sex is; their age; whether they are married; ask them what their interests are. From the paradigm of a privacy advocate–or

49. *See* 5 U.S.C. § 552a (1988); *see also* Privacy Protection Study Commission. Act Dec. 31, 1974, P.L. 93-579, § 5, 88 Stat. 1905, as amended by Act June 1, 1977, P.L. 95-38, 91 Stat.179.

50. By the time women gained the right to vote in 1920, corporations had acquired 14th Amendment equal protection and due process rights, 5th Amendment rights, and 4th Amendment rights.

someone sensitive to privacy issues–these are supremely bad ideas. There is really no need to know that information and so one should not convey it.

The OECD privacy guidelines contain other strong protections. The guidelines include issues such as data quality–the idea that if you are going to collect data and you are going to use this data to make decisions about people, it better be right. This includes the right of individuals to inspect the data. There are also provisions for purpose specification–the idea that information collected for one purpose should not be used for another purpose. And this is important in the commercial sphere where more and more information collected for transactions is also used for building consumer profiles. There are security safeguards–real provisions–saying that if you don't keep your information secure, individuals can have a remedy in court. There are principles of openness–the idea that government or commercial entities alike should not keep secret databases. This has a large effect in preventing people from creating personal databases. It also harkens back just to principles of fairness, that people should know that information is being collected about them, and that in an open society secret databases are intolerable.

OECD calls for individual participation in the collection of personally-identifiable information. And that participation can be opt-out choice or opt-in consent. From the privacy advocate's perspective, consent is really the only way of dealing with these issues. I've been working on analogies to try to illustrate the opt-in vs. opt-out debate. Opt-in meaning you assent, that you approve versus what the industry will call as choice, where they choose for you. Opt-out or negative options are bizarre methods for securing a right. For instance, we have the right to be free personally from attacks. We have notions of the common law tort of battery. A battery is a touching: an unauthorized touching. And it doesn't have to be very serious. You can batter someone by just touching them and not causing harm. What if American law afforded us protections from battery on an opt-out basis? The result would be absurd. On the other hand, opt-in makes sense and we use it in our daily dealings with others. When you go to the doctor and you have elective surgery, you sign a form that is a consent to a battery–you opt-in. You say, "Okay doctor, you can touch me in this way and perform this surgery." We should

have a similar system for collection of personal information. Before others can collect and use it, they should secure individual consent. Currently, we allow people to take personal information from us because they can. In other areas of our substantive political rights, we would never allow opt-out.

So the OECD privacy guidelines provide great protections for people in Europe. We have not thus far found protections like that in the United States, except in very small sectors. Professor Bartow pointed out the Video Privacy Protection Act–in fact, it is opt-in–and it is a transactional opt-in.[51] So if you go to the video store and you rent a film, if they want to sell information based on your rental, they have to ask every time. So what is interesting is that in the United States you, in fact, have more right to privacy in your video rental records than you do in the amount of money you have in your financial accounts.[52] You have more privacy in the fact that you rent *Bambi* than your medical records.[53] Sectoral approaches to privacy–ones that specify protections for certain types of data in defined circumstances–produce these absurd results.

We are living in an era of privacy self-regulation in the United States. And it has always struck me as kind of obvious that privacy self-regulation doesn't work where the self-regulated industry benefits from violating your privacy. The economists haven't been able to figure this out, but companies have very strong interest in violating privacy in collecting consumer information. And we can't expect them to self-regulate. In fact, they haven't. I did want to also comment on the majority leader, Dick Armey–we work with Dick Armey at EPIC on governmental privacy issues where he is a very strong advocate of protecting personal information from government collection. However, in the private sector he has penned a number of essays with an interesting argument. And the argument always ends with

51. *See* Bartow, *supra* note 3, at 665. *See also* The Video Privacy Protection Act, 18 U.S.C. § 2710 (1994).

52. The Gramm-Leach-Bliley Act allows financial institutions to share personal information, including bank account balances, with others on an opt-out basis. 15 U.S.C. § 6801 (2001).

53. The Health Insurance Portability and Accountability Act Privacy Rule allows marketing based on individually-identifiable health records. Some types of medical marketing are considered "education," and the individual has no right to opt out. 45 C.F.R. 164.501.

the same conclusion regardless of the underlying facts: that we shouldn't regulate the private sector on privacy. Earlier this year he argued that our economy is strong and we don't want to mess up our economy, so we don't regulate the private sector on privacy.[54] Now that our economy has taken for a downturn, we have a different premise, the premise that people aren't making as much money as they were. If we regulate privacy now, it is going to harm the private sector. So we have this kind of all-encompassing argument that always supports privacy self-regulation regardless of the underlying premises. But at the same time, Professor Bartow is right. Dick Armey has been on the forefront of regulating the Internet in other ways–in attempting to prohibit sexual content.[55] The United States actually has the most intense proponent of Internet regulation. I don't think there is a westernized nation that has regulated Internet more than the United States.[56]

Just because there isn't government regulation doesn't mean there isn't some type of Internet regulation. The question is who is doing the regulating? Is the regulating being done by a government body that is subject to oversight? Or is it being done by a private entity, like Cisco, Microsoft, AOL, or Hewlett Packard. Technology companies regulate the Internet by affecting its architecture.[57] For instance, Cisco has a white paper that describes a router that can discern the difference between different types of content, and then discriminate against unsponsored content.[58] And we're likely to see such routers employed where companies provide both content and connection to

54. John Schwartz, *Fears on Privacy Law Spur Warning by Armey*, New York Times, Apr. 9, 2001, *available at* http://www.nytimes.com/2001/04/09/technology/09PRIV.html (last visited Aprl 14, 2002).

55. Representative Armey voted in favor of the Communications Decency Act of 1996, which was found unconstitutional by the Supreme Court in *Reno v. ACLU*, 521 U.S. 844 (1997).

56. *See e.g.*, Children's Internet Protection Act, *supra* note 13; Child Online Protection Act, 47 U.S.C. 231 (1998); Communications Decency Act of 1996, *supra* note 11.

57. LAURENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (June 2000).

58. *See e.g.* Center for Digital Democracy, *Open Access available at* http://www.democraticmedia.org/issues/openaccess/index.html (last visited May 8, 2002); Center for Digital Democracy, *CISCO 1999 White Paper: Controlling your newtwork—a must for cable operators, available at* http://www.democraticmedia.org/issues/openaccess/cisco.html (last visited May 8, 2002).

the Internet. A company, such as AOL, can say: "This is AOL content, I am going to speed it up. This is content from a competitor, I am going to slow it down." This type of private regulation is completely uncountable.

Consumer Rights Management (CRM) is a field that greatly affects personal privacy, but is unregulated. I don't like to use the word CRM because it is euphemism for a less friendly term: profiling.[59] It is immense in the United States. In fact, if you have ever bought something from a catalog, 90% of catalog companies will report all sorts of information about your purchase; your name, your address. If you buy clothes, they will report your clothing size. These are all built into these enormous databases. Some of them are maintained by credit-reporting agencies, and they know a lot about you on a personally identifiable level. They know your social security number. They know your sex. They know whether or not you are married. They know whether or not you have children. They know your religion. They know what books you are interested in. They know whether you are susceptible to certain type of scam marketing. And you have only a limited right to access this information. On the other hand, the Privacy Act allows you to write to the FBI and say I would like to see my FBI file. And the FBI would be compelled to reveal the file. Very few of us in this room have an FBI file. But I will guarantee you every one of us has a file maintained by all three credit-reporting agencies that not only reports on credit, but also reports on your consumer buying habits. You would also have a ChoicePoint file that tracks numerous aspects of your life from public records databases.[60]

There are other issues that will have serious impact on the future. One of them is Digital Rights Management (DRM).[61] DRM limits access to digital files. But in doing so, they often link your identity to content. So we are operating in a system where there are companies that are unregu-

59. EPIC maintains a comprehensive web page on profiling online, *available at* http://www.epic.org/privacy/profiling/ (last visited April 14, 2002).

60. EPIC has filed a series of Freedom of Information Act (FOIA) requests and brought suit against the Department of Justice to learn more about the ChoicePoint database and how ChoicePoint dossiers are sold to the federal government. *See* EPIC v. Dep't. of Justice & Dep't. of the Treasury, No. C.A. No. 02-0063 (D.D.C. 2002), *available at* http://www.epic.org/privacy/litigation/ (last visited May 8, 2002).

61. EPIC maintains a website on Digital Rights Management and Privacy online at http://www.epic.org/privacy/drm/ (last visited April 14, 2002).

lated that can track what you consume, what books you read, what music you listen to without limits on the collection, use and transfer of personal information. In fact, if a public library attempted to do the same thing, it would violate the First Amendment. Librarians are some of the biggest advocates of privacy in history. They have developed systems that expunge circulation records so that your identity cannot be linked to content.[62] Content owners, however, are not respectful of privacy, and will use DRM systems to track content consumption and profile individuals.

Location privacy is likely to emerge as an important issue. Because of the FCC mandate, cell phones are now designed with technology that can track the location of the caller when "911" is dialed. This really makes a lot of sense. Often times you might be in an accident, you might be confused. You might not be able to tell the operator where you are. Well, your phone will, and this is a great innovation. But what has happened is, on the wings of this good innovation, a number of commercial entities have flown in to provide location-based services that track you. So, in absence of regulation, the day will come where you are walking down the street and your phone will deliver an instant message that says: "Save 50 cents at Starbucks now", and you'll turn around and you'll be next to a Starbucks. The potential for profiling is going to be immense. And it is not only profiling based on your activities–I have a cell phone. The panelist next to me might have a cell phone, as well. A marketer can then build a relationship between our proximity and deduce that we are friends or acquaintances. We can then be profiled based on the fact that we associate with each other on some level.

I see the corporate logo for Verizon flashing up on the conference screen here. Verizon is active on one aspect of privacy that many people have never considered, and that is called CPNI, Customer Proprietary Network Information. Every time you pick up the telephone to make a call, the telephone company has the ability to log whom you called and when. And the different telephone companies, Verizon being one of them, are trying to sell this information.[63] We

62. *See* Code of Ethics of the American Library Association, *available at* http://www.ala.org/alaorg/oif/ethics.html (last visited April 14, 2002).

63. EPIC maintains a website on Customer Proprietary Network Information online at http://www.epic.org/privacy/cpni/ (last visited April 14,

are challenging this. This is another area where people expect their telephone communications to be private.

Let me shift gears, in the remaining minute and a half, to talk about government incursions into privacy. We have seen since 9/11 a number of defense companies racing to turn surveillance technologies developed for use against our enemies on to Americans. And we are seeing an increased willingness amongst Americans to be subject to these surveillance technologies.

Carnivore is one surveillance technology that is likely to be used more frequently. And EPIC has been involved in extensive Freedom of Information Act litigation to learn more about the Carnivore system.[64] Carnivore is one of the methods that federal law enforcement uses to wiretap the Internet. It is actually a freestanding computer that is taken to the Internet service provider. And it monitors all your communications, whether it be e-mail, chat, web-browsing habits. In doing so, it engages in what we term as a general search. Carnivore grabs everyone's information on the ISP. So, if I were online using a certain ISP, and the law enforcement wanted to capture my Internet communications, they would install Carnivore at my ISP. In doing so, they also collect everybody else's e-mail and web-browsing habits in order filter through to get mine. We are arguing that the FBI has inadequate internal controls to use Carnivore and that the system engages in a general search that is constitutionally impermissible. We have argued that the ISP themselves should do the monitoring, when there is a need to collect information on an Internet user.

We've also seen other technologies developed since 9/11. We've seen ideas about national ID.[65] Alan Dershowitz wrote an excellent column in the New York Times about national ID.[66] But his idea of national ID looked more like a frequent flyer card than what a national ID looks like. And we also have Larry Ellison from Oracle, who is running

---

2002).

64. EPIC maintains a website on Carnivore online at http://www.epic.org/privacy/carnivore/ (last visited April 14, 2002).

65. EPIC maintains a website on national ID systems online at http://www.epic.org/privacy/id_cards/ (last visited April 14, 2002).

66. Alan M. Dershowitz, *Why Fear National ID Cards?*, New York Times, Oct. 13, 2001 *available at* www.nytimes.com/2001/10/13/opinion/13DERS.html (last visited April 14, 2002).

around saying that he will donate the databases–in fact, he's been trying to do this for a long time. He has been trying to sell a national medical database system to the American government, and he now thinks he can sell this database under the guise of national security. I should be clear about what a national ID is. A national ID has historically been used by repressive governments to track people and deny them participation in events, the enjoyment in services, and travel. National ID was used by the Nazis; it was used by the South Africans to keep apartheid in place. Documentation in general–identifying people in general–has always been a system of social control or a way to build identity. I think the first census, of course, was in the Book of Numbers in the Old Testament.[67] And that was an effort of Moses to build an identity, to classify people. The slave south, of course, had document requirements where slaves had to carry a document at all times identifying who they were, and thus limiting their travel. So ID has a history of being a method of social control. And we think of national ID, it necessarily has to be mandatory. It can't be optional. And it is going to require the creation of databases to track your movements, and probably your financial transactions as well.

What I would like to close with is facial recognition. Facial recognition technology purports to either identify a person from a crowd automatically or verify an identity based on facial structure. Facial recognition technology has been applied here and there–we saw it at the Super Bowl last year. And as with other invasive technologies, it is always justified by some enormous risk. The people who applied it at the Super Bowl said they needed it to detect terrorists. They, in fact, caught none. They identified a bunch of pickpockets and petty criminals. The UK created a surveillance infrastructure for the interception of terrorists, but in fact they have never caught a terrorist in the UK despite having three million cameras. So we have new systems out there that not only will monitor your activities in public, they will link your identity to your activities in public. And that is fundamentally going to change the way public space could be viewed.

---

67. Numbers 1:1-2 (New International Version) ("Take a census of the whole Israelite community by their clans and families, listing listing every man by name, one by one.").

Let me conclude by illustrating some ways in which one can protect their personal information. Most importantly, try to limit the amount of personal information that you give out. I tell people that they should engage in privacy self-defense. When organizations such as The New York Times websites requires you to give information, give them fake information. It's also important to opt-out of information sharing to the fullest extent possible. You can also use encryption.[68] It is an effective way of hiding many communications. And there are also a number of anonymizers out there that can mask your Internet browsing. On EPIC.org, we have a page devoted to privacy-enhancing tools, and I encourage you to visit it. With that, I look forward to questions and answers. Thank you for your time.

GARY M. SCHOBER: Thanks, Chris. A couple years ago, for Christmas, I purchased–for my daughter–the life story of Mia Hamm, one of the very best soccer players today. And at the same time, I purchased for my son the life story of Derek Jeter a pretty good ball player for the New York Yankees. I got both of them through Amazon.com. Now whenever there is any type of sports book available, I get an e-mail from Amazon.com saying, "Hey, Schober, you missed this one. Why don't you buy this book as well?" That can be a little annoying, but it is not the end of the world. I can delete the message from amazon.com or I can look at it if I want. In either case, it's pretty obvious that Amazon.com knows that I have an interest in sports books. They can begin to create a profile on what interests me. Remember I told you a little bit about my colleague who got caught looking at a porno site? You can imagine what they know about him. Also, remember his reaction? He was more than annoyed, he was angry that we learned something about him that was or should have been private. I assume a lot of his reaction was embarrassment. Well, all of these things can be minor annoyances when compared to the employer or anyone else having access to another person's medical history. I am not ashamed to say, I've had some procedures I don't want you to know about, no less my employer. To

68. Junkbusters Corp. has a free service called "Declare" that will allow individuals to opt-out of many profiling databases at http://www.junkbusters.com/declare.html (last visited April 14, 2002).

talk about this problem, we're now going to turn the floor over to Phyllis. Phyllis.

PHYLLIS BORZI: Thanks, Gary. This is perhaps to me one of the more frightening aspects of the whole privacy issue. As Ann pointed out at the beginning and Chris talked about as well, the personal health information of every American and the extent to which it can be accessed by other people is governed really by a patchwork of state and federal laws. I will use the word patchwork because that is what it is, although some patches are larger than others. And these laws govern the kind of healthcare information that moves in and out of cyberspace, across state lines, across national lines, between hospitals, providers offices, insurers, and other third party payers. And, of course, included in this group is your employer. Most Americans, 85% of all Americans, get their health insurance through their employers. And in many cases, the employers have access to what is called "Protected Health Information" or PHI.[69] That is information which all of us could easily identify as personally identifiable health information. Under our current patchwork system of regulation, PHI can be distributed–can be used and disclosed–without notice to the person who is the subject of the information, certainly without that person's consent, and for reasons that have absolutely nothing to do with the purpose for which that information has been collected, namely, a patient's treatment or the payment for that treatment.

A simple example–a couple of simple examples: how many of you have ever gone to have an x-ray or some other diagnostic test? When you arrive at the reception counter, they give you a whole bunch of papers to fill out–of course the first thing they want is your insurance card–but then you have a whole bunch of papers to fill out. And of course, being trained as a lawyer, I stand there and read them all and the person at the counter gets angry at me for wasting time in the line. The person usually just says, "Sign all

69. This terminology is used in the recent U.S. Department of Health and Human Services Final Rule on medical privacy under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). *See* Press Release, Health and Human Services News, H.H.S. Announces Final Regulation Establishing First-Ever National Standards to Protect Patients' Personal Medical Records, *available at* www.hhs.gov/news/press/2000pres/20001220.html (last visited May 8, 2002).

these," and typically I respond with, "What are they?" And they say, "Oh, well, you know it is just an assignment, basically a paper that allows us to go to your third party payer and collect money." But if you really read those documents, what they also give the medical provider carte blanche to do is to take the medical information that they gain as a result of those tests and use them for whatever purposes they want. The kinds of statements that Anne alluded to and Chris talked about, are on all of these medical papers.

Now, you have a choice of whether or not to sign away your privacy rights. I can decide that I am not going to have that chest x-ray, and then I don't have to sign all of these papers. But to say that this is an opt-in or a voluntary decision on my part–to waive any of these shreds of the patchwork of privacy protection–I think is probably kind of a stretch. The difficulty, of course, is we never do know – as Anne and Chris have pointed out–with whom is this information is being shared. If it is shared with lenders, it could ultimately find its way into your credit file, we know. And more often than not, it could find its way into the personnel files of the employer.

The states have grappled with this question for fifty years or so. And many states have state privacy laws. The difficulty with them, like the difficulty with the federal law that I am going to talk about in a minute, is that the protection provided under them is imperfect. In fact, probably to call these laws Swiss cheese would be an overstatement of their strength. There are broad exceptions in all of these state laws for public safety uses, which probably means that they would allow the collection, Gary, of your EZ-Pass information–the kind of stuff that you collect through an EZ-Pass.

Of course, the medical equivalent of EZ-Pass is your insurance card. The kind of information that is collected when you use your insurance card can be shared with anybody that is broadly described as involved in public safety or public health.. Because your employer pays the bill, your employer often can get access to this information as well.

Recently I had occasion to look at a couple of the state laws in the context of some part-time consulting work I did for the U.S. Department of Health and Human Services (HHS) while they were working on the Final Rule on

medical privacy that was issued at the end of 2000. I wear so many caps that I need a hat rack for them, but my two major caps, as Gary pointed out, are that I am both a research professor in the School of Public Health and Health Services at George Washington University and also a practicing lawyer. I was hired by HHS in my research professor capacity.

But in my private law practice, I represent employee benefit plan sponsors: unions, employers, employee benefit plans. And so I have some hands-on experience with claims data and PHI. Most of those employers and most of those unions provide health benefits but they don't administer the benefits themselves. They hire a third party, an outside administrator. So they have a limited access, except if they want to, to the actual medical claims information. But some of my clients actually administer their own claims in-house. Many very large companies do that as well or at least they have people in their Human Resources Department that oversee outside administrators and have the ability to access this information.

When HHS was writing these privacy regulations I was hired because they were concerned about some of these employment-related issues and they sought some outside expertise to assist them. A major focus of my work was to read through some of the comments.

Let me step back and give you a bit of an overview first before I talk more specifically about these regulations. Congress was concerned about the lack of privacy protection for medical information. So Congress tried to address these issues through some provisions in HIPAA, a federal law called the Health Insurance Portability and Accountability Act of 1996.

You probably know about HIPAA because of the publicity surrounding the so-called "portability" or insurance provisions–provisions in the law that said that if you are continuously covered under a health plan, you can't be denied coverage when you move to a new employer because of a pre-existing condition and put limitations on the amount of waiting time you might have in a new health plan for a pre-existing condition. But an important part of HIPAA was the section called administrative simplification. And that really is the part of the Act that I am going to talk about today.

Under the administrative simplification rules, there are

a variety of types of regulation that HHS is supposed to issue, including a final regulation issued by HHS dealing with electronic data interchange. Certain basic transactions, such as paying claims, have to be undertaken by all people who engage in those electronic transactions in standard form, using standard datasets, etc. One of the more controversial issues that delayed Congress' consideration of this broad area, and certainly the agency's issuance of a regulation on the topic, is the question that Chris talked about a minute ago: the adoption of a unique identifier for each individual. The whole purpose of this administrative simplification initiative is to establish uniform datasets so that everybody's medical information can be accessed simply and easily in comparable form.

If I were to walk out of this building onto a busy street–I assume there is a busy street out there someplace–and I walked out and was busy chatting with my colleagues and didn't watch where I was going, I could get hurt. Suppose I was wiped out by the nearest truck and the EMTs took me to the nearest trauma center.

The theory here is the medical personnel could put in my unique identifier–some people have suggested it be the social security number–but they could put in the unique identifier and push a button, and within a microsecond, the ER staff could access all of the medical information about me. So they would know what my previous medical history has been, what medicines I am allergic to, if I have any particular peculiar health considerations.

From a medical efficiency and quality of care point of view, this makes a lot of sense. I can get better treatment and I don't have to worry about drug interactions, etc. So the good news is the clinicians could press a button and get all the medical information that relates to Phyllis Borzi. Of course, that bad news is they could push a button and get all the medical information that relates to Phyllis Borzi because who knows who could push that button, and who has access to that information.

So Congress passed HIPAA and at the same time that it created these electronic data information interchange rules, it required the Secretary of Health and Human Services to propose legislation–or at least to come up with legislative recommendations–within a year of the enactment of the law. And Congress was expected to adopt legislation addressing privacy and security protections. But the security

regulations haven't been issued yet, but we keep waiting–it is like "Waiting for Godot"–we keep waiting and waiting and hearing they're coming "soon".

Actually I chaired a program on health issues last Thursday and Friday and I had somebody from HHS on my panel. And I asked her to define "soon" and she said that these regulations were actually pending at the Office of Management and Budget (OMB) waiting for clearance. Of course, we in Washington call that the ultimate black hole. Who knows when OMB will release them?

So the Secretary was directed to issue legislative recommendations on medical privacy. She had a year to do it. And Donna Shalala, who was the Secretary at the time, in fact, met the deadline, at least by Congressional standards. She was a couple months late, but she basically came out with recommendations that everybody hated.

Now in one of my previous lives, I was a Congressional staff person for the U.S. House of Representative for sixteen years. And I always figured when my bosses came up with a legislative proposal that everybody hated, they were probably on the right track. Because the difficulty, of course, is resolving the tension between all the different interests. But everybody hated her proposals which many people thought meant that Congress would then, in the two years it had given itself to adopt legislation in this area, overcome its natural inertia, confusion, tension and politics and actually pass something. But, of course, that didn't happen. Congress in the original HIPAA statute anticipated that the Secretary would make recommendations–that Congress would fail to adopt a law implementing, overturning, or modifying them. And if that scenario came to pass, which of course it did, the statute then directed the Secretary to finalize her recommendations as regulations, which she did. In 1999, HHS issued proposed regulations.[70] In response to the proposed rule, HHS got more than 52,000 comments. And the privacy rule was finalized on December 28, 2002.[71]

Now let me just say a word about comments. As I said, I worked on the Congressional staff for sixteen years. We got a lot of form letters, form post cards, or other organized communications. Often people try to generate a lot of

70. 64 Fed. Reg. 59918 (Nov. 3, 1999).
71. 65 Fed. Reg. 82462 (Dec. 28, 2000).

interest on a particular side of an issue by organizing the grass roots–and I am a big grass roots' fan, so I am not trying to minimize the effect of grass roots lobbying. When I was hired as a part-time consultant by HHS, one of my jobs was to go through the comments that had been filed where people responded to some of the privacy concerns related to employment-related issues: worker's compensation, disease management, fitness for duty exams–all the things that employers do in the workplace using PHI. Probably about two-thirds of all the comments touched on those issues.

And I will tell you this: remarkably, while the comments did include some form letters, by and large the comments were individually written. Many of them, of course, were submitted by trade associations or companies.

But what was remarkable about reading those comments–and by the way, if you want to look at them, they are online on the HHS website–what was remarkable about those comments was the richness and the diversity of the comments that came from regular, ordinary people.

Now I don't know how many of you in the audience keep the Federal Register by your bedside or who have read the Federal Register at all, but you probably know that the way regulations are issued, of course, is that the issuing agency sends the regulation to the Federal Register with a notice soliciting comments. The business community typically has people who monitor this stuff, and they know that they can comment on the proposals, so they file comments.

Regular ordinary Americans don't generally know about this procedure, but as a manifestation of how important medical privacy issues are to people, the popular press picked up on the notion that HHS had issued proposed rules on medical privacy. You could see it on all the news magazine shows; you could see it on the local news. Probably all of you knew that something was going on with medical privacy. So there were lots and lots and lots of comments regarding privacy in response to the HHS proposals, and, as I said before, the Secretary finally finalized the privacy regulations at the end of December, 2000.

The regulations cover, really, several broad areas. The first thing that the regulations cover is how personal health information can be disclosed or used. So it has restrictions on disclosure and use of PHI. It also establishes–and to me this was the important part of the regulation, almost as important as the restrictions–the final privacy rule gives

individuals, for the first time, federal rights to their own medical information. This is a big deal.

I'll tell you a little story. When I first came to the School of Public Health in 1995, I was working on a research project on various aspects of the expansion of managed care to the Medicaid population.. I do a lot of research in those areas. And I had a young graduate student who was working on a project come to me and ask "Who owns medical information?" And I said, "Good question." He said, "I think, isn't it the patient that owns the medical information?" And I said to him, "Well, where have you looked to find the answer to that question?" He said, "Well, I just came to your office to ask you this question." I said, "No, no. You are a graduate student. You have a research position, you need to do research." I told him to research the question and come back and tell me what he found. So he disappeared for several days. And when he came back, he said, "You know, I couldn't find anything." And I said, "Well what did you look at?" And he told me all the usual secondary sources of information that students love to browse: Medline, and some of the health periodicals, etc. And I said, "No, No, No. You need to look at state law. You need to look at who, under state law, has the ownership rights." And so he went away for another couple days. And he came back and said, "You know what? I don't own my own medical information. It is owned by the provider who puts together your medical records." And he was outraged by this.

I don't know how many of you have ever tried to have your medical records shifted from one provider to the next, but it is very difficult to get people to move that information. But most people think that they own their medical information. Not only do they not own it, they generally don't have access to it. And that is one of the reasons that, if you do get your provider to allow you to move your medical records, they frequently will require it to be a provider–to–provider transfer, not just handing over to you all your medical records–some providers will do that, though. Importantly, the new rules provide federally protected rights for individuals regarding protected health information, which I will talk about in a second. And then

they create special rules for employers,[72] and people who provide services to health plans.[73]

The regulation, like HIPAA itself, applies only to covered entities. And the covered entities are three. They are health plans; they are health care providers–the people who provide direct treatment to you; and there are things called health care clearinghouses, which primarily exist as translators, which in the new electronic data interchange mode, turn non-standard transactions into standard ones, or vice versa. Notice what is not in the covered entity group: many people or organizations who today have access to your medical information but who are not reached under this regulation. And chief among them are people like employers, workers compensation carriers, life and disability insurance carriers. All of these other insurance functions use medical information as a way to make their benefit determinations. And yet, they are not covered under these privacy regulations.

When I talk about this regulation with my students, I try to get them to understand the contextual framework for the rule. And what I say is that Congress drew a box and in the box are the covered entities: the health plan, the health care providers, the health clearinghouses. And all the PHI is in the box. Everybody else is outside the box.

A lot of people spent a lot of money, like the workers compensation and other insurance carriers, to make certain that they would not be subject to these privacy regulations. They lobbied successfully to be outside the box, because what they thought if they were outside the box, then they could continue to do their thing with PHI without being subject to any new rules.

But when Congress drew its HIPAA box, it put all the PHI inside. So if you are in the box, that is if you are a covered entity, you can use or disclose PHI freely for three–without any consent or authorization as a general manner–

72. Special rules are provided for group health plans that plan to share PHI with employers and other plan sponsors provided that certain conditions are met. *See* Privacy of Individually Identifiable Health Information, 45 CFR § 164.504(f) (2000), 65 Fed. Reg. 82809 (Dec. 28, 2000).

73. Special rules are also provided for "business associates". Business associates are persons who provide certain services to or on behalf of the covered entity, including legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services. *See* 45 CFR § 164.504(e)(1), 65 Fed. Reg. 82808 (Dec. 28, 2000).

for three permitted purposes. The purposes are treatment,[74] payment,[75] and health care operations.[76]

These terms are defined in the final privacy rule, but we don't have enough time for me to describe the trucks that you can drive through the definition of health care operations because it such a broad term. But suffice it to say, it covers things like grievances and appeals, quality improvement, underwriting, claims payment, etc.

If you are a covered entity and in the box, you can use this information for treatment, payment and health care operations with respect to the covered entity. And covered entities inside the box can disclose PHI to non-covered entities (that is those outside the box), but only for those three purposes. But if any of those entities outside the box need PHI held by any of those covered entities in the box to use in carrying out their own operations, the only way a non-covered entity could have access to the inside-the-box information is by getting an individual authorization from the person who is the subject of that individualized medical information.

Moreover, the final privacy regulation specifically knocks out the kind of general waivers that most health care providers and institutions use today, because the individual authorization has to be very specific. It has to say who has the right to get the information, for what purposes, and for how long. It has to have an expiration date and it has to tell the person who is being asked to sign that he or she has the right to terminate the authorization.[77] So it is a great protection.

Of course, the final medical privacy rule also causes disruption because a lot of these entities that are outside the box need PHI to carry out their legitimate functions too. So what the regulation also does is create a mechanism through which certain of those entities can get access to PHI. If you are the employer, or if you are the lawyer who represents these companies or health plans and you want access to that information because you need to perform vital functions for the covered entity, you need to be able to get that information.

---

74. 45 CFR § 164.501, 65 Fed. Reg. 82805 (Dec. 28, 2000).

75. 45 CFR § 164.501, 65 Fed. Reg. 82804-05 (Dec. 28, 2000).

76. 45 CFR § 164.501, 65 Fed. Reg. 82803 (Dec. 28, 2000).

77. *See* 45 CFR § 164.508(c), 65 Fed. Reg. 82811-12 (Dec. 28, 2000) for the rules on authorizations.

As I mentioned previously, the final privacy rule provides mechanisms for some non-covered entities who are outside the box to, in essence, get into the box.

First, if you are the employer who sponsors a group health plan, you can take advantage of the special group health plan rules if you meet certain conditions.[78] One of the major ones is that the plan documents have to be amended and the participants in that plan have to be notified who among the employers' employees are going to have access to PHI, what information they are going to have access to, and what functions they perform for which PHI is necessary.

The concept of minimum necessary that Chris talked about a few minutes ago is an integral part of this regulation. You can't generally just have access to somebody's entire medical history or medical record. The access has to be tailored only to the kind of information necessary for you to perform the function.

If you are somebody like me, a lawyer who is plan counsel, or if you are a utilization review company, a third-party administrator that handles claims, etc., you must have a contractual relationship with the health plan, as a business associate. There are a number of very specific provisions that must be in the business associate's contract in order for the covered entity to share PHI with the business associate.[79]

And what both of these types of structures do–the employer/plan sponsor special rule and the business associate contract requirement–is create a mechanism, so that those folks can get in the box. Most significantly, these mechanisms are legally enforceable and both employers and business associates have to agree that when they receive PHI from covered entities pursuant to the special rules, they will be bound by the same rules that apply to the people who are already in the box because they are covered entities.

Now let me jump to the special rules for individuals because I think they are really quite important. First of all, an individual has the right to have access to his or her medical records and to inspect and make a copy of those records.[80] In addition, an individual has the right to correct

78. *See* 45 CFR § 164.504(f), 65 Fed. Reg. 82809 (Dec. 28, 2000).

79. *See* 45 CFR § 164.504(e)(1), 65 Fed. Reg. 82808 (Dec. 28, 2000).

80. There are three exceptions to this rule. Individuals do not have a right of access to: (1) psychotherapy notes, (2) information compiled in reasonable

his or her own medical records if there are errors in the medical records.[81] As a practical matter, that means that individuals can demand that additional material disputing what is in the record be included in the record. Significantly, individuals have the right to notice that their PHI will be used by covered entities,[82] and, if the covered entity takes advantage of the special rules which permit disclosure to employers and business associates, how those entities are going to use their information. So some of the fair information practices approach to privacy protections that Anne talked about in the EU countries are incorporated in the final privacy rule. You also as an individual have a right to an accounting of who has gotten your medical information for the prior six years before you make this request. Only routine uses–treatment, payment, health care operations–are exempt from this.[83] But if they give your medical information to anyone else, you have a right to demand an accounting. And you also have a right, under these new federal regulations, to complain to the privacy officer of a covered entity–each covered entity is required to have one–if you believe your rights under the final privacy rule have been violated. [84] In addition, you have a right to demand that the Secretary of HHS investigate any complaints. HIPAA does impose heavy criminal and civil penalties for violations of privacy. But the difficulty with these penalties and the problem with the whole structure of the regulation is that Congress only gave the Secretary the right to impose penalties on covered entities. And the major source of Congress' concern about medical privacy is the problem caused when PHI gets into

---

anticipation of, or for use in, a civil, criminal or administrative action or proceeding, and (3) certain protected health information maintained by a covered entity that is subject to or exempted from the Clinical Laboratory Improvements Amendments of 1988 (CLIA). 45 CFR § 165.524(a), 65 Fed. Reg. 82823 (Dec. 28, 2000).

81. 45 CFR § 164.526, 65 Fed. Reg. 82824 (Dec. 28, 2000).

82. 45 CFR § 164.520, 65 Fed. Reg. 82820-22 (Dec. 28, 2000).

83. 45 CFR § 164.528, 65 Fed. Reg. 82826 (Dec. 28, 2000). Covered entities must provide this information within a reasonable time after the request is made, generally no later than 60 days following the receipt of the request, although under certain circumstances, extensions may be allowed.

84. See 45 CFR § 164.530(a), 65 Fed. Reg. 82826 (Dec. 28, 2000) (requiring each covered entity to have a privacy officer) and 45 CFR § 164.530(d), 65 Fed. Reg. 82827 (Dec. 28, 2000) (requiring each covered entity to establish a complaint mechanism).

the hands of the employer and potentially affects the employment relationship.

Employers basically wear multiple hats. They operate as employers, but they often have people in their Human Resources Department or Personnel Offices who administer, or at least interact, with the people who administer their employee benefit plans. In some cases, the employers actually administer their health benefit plans or some of the features of those plans in-house. As employers, of course, they have responsibilities for hiring, promotion, termination, etc. And while it is true that under the law employers can wear many hats, what is really hard to figure out is what hat are they wearing at the point that they acquire this confidential medical information.

Now, let's focus on Gary's example about an employer performing a normal employer auditing function of the e-mail system and the Internet system and discovering that an employee is looking at websites related to baby merchandise and through that audit discovers that employee is pregnant. Presumably the person who is in charge of that audit acquires that information, not because he or she has access to confidential medical files, but because he or she was performing another function. Under the final privacy rule, information that an employer acquires wearing another hat (that is, not its covered entity or group health plan hat) is not a problem. The bigger problem, of course, is when you are an employee of the employer who is both the HR person who monitors Blue Cross Blue Shield claims information and the HR person who monitors new hires, and you acquire individual information about someone's medical condition. Let's say Gary's employee comes to him and wants to take a family and medical leave. And we know under the Family and Medical Leave Act, there are circumstances in which an employer could ask people seeking leave to provide medical information. What happens to that medical information? In what context has the employer acquired getting that information? And what does the employer do with it? So there are a lot of questions.

Another big area of concern regarding the privacy of employee's medical information comes up in connection with disease-management programs that many employers are putting in to place. Employers are putting them in to place for very good, positive reasons–they want to improve

their employees' health and improve their productivity. Of course, employers also want to reduce their over all medical costs because if you get employees involved in some of these focused disease management programs–cholesterol screening, tobacco cessation, etc.–employers can actually improve their employees' health outcomes and reduce their ultimate medical costs. But in order to figure out who should be in that program, most of the time what the employers do is health profiling. Now, some of the profiling doesn't need to be particularly sophisticated–I am clearly overweight, my employer could target me, just by looking at me, for a weight-management program. But it isn't so obvious which employees could use a cholesterol-management, or a blood pressure reduction program. So when employers use profiling techniques to identify people, the use of the PHI held by the covered entity (group health plan) for other employer or benefit purposes is problematic from a privacy point of view.

One of the big problems is drawing the line between trying to improve the health of your employees and marketing. I guess it was about two years ago, maybe a little longer–there was a big story on the front page of The Washington Post about a major drugstore chain, CVS, having sold information regarding their customers to drug companies. Many drug companies now do direct marketing of their drugs to individual consumers. And what CVS did, apparently, was to sell its list of people using certain cholesterol-lowering drugs or diabetes-management drugs to drug companies producing rival drug to those which had been prescribed. Suddenly, CVS customers got, at home, marketing information from certain drug companies asking them to talk to their doctor about changing over to their products instead of the ones that had been prescribed. And there was a big to do about this in The Washington Post, as well there should have been, because that was a very, very serious misuse of confidential health information.

So the bottom line is this: the advantages of our increased technology also have down sides. And the difficulty in the area of confidential medical information is it is impossible to put the genie back in the bottle. Once there has been a compromise of your medical privacy information and that information has been made public, how in the world can you remedy it? Oh sure, you can impose a civil fine on the culprit who discloses it, assuming

you can identify him. But what does that mean, when your medical information has been disclosed and could conceivably be used for a wide variety of non-medically related things? Medical privacy is an area that bears watching closely And it is very, very interesting. Thank you.

GARY M. SCHOBER: Thank you, Phyllis. That was great. First, I'm going to ask the speakers to put on their microphones, if they haven't already. Now it is that time when we get to open up the floor to you. Any questions?

Yes sir. While he is walking down to the microphone– Phyllis, do you sleep with the federal register near your bed?

PHYLLIS: No, I usually leave it in the trunk of my car.

GARY: Whoa, that was close.

QUESTION: I have a question for you, Mr. Schober.

GARY: That's not allowed.

QUESTION: I was fascinated by your story of the transgression of yours on the Washington Bridge. I teach mathematics here at UB, and just last week I was telling my calculus class about a very famous theorem in mathematics which says, in effect, that if your average speed during the trip is 80 mph, then there must have been an instant in the trip when you were driving precisely 80 mph. And I said to the class, "You know it seems to me that raises some interesting legal questions. The law accepts evidence of fingerprints and DNA, and maybe even holographs some day, but does the law accept as evidence mathematical or other scientific theories?" I could imagine that in computer science there may be a result that says if your database has certain general features, then maybe it has certain specific features and perhaps that could be used to prove that you logged on to a naughty site. So, I am just wondering, does the law accept sort of general theoretical scientific theories as evidence for this or that?

GARY: As it turns out, in my prior life before I went to law school, I was a math major and worked for an

engineering firm for a number of years as, what they called, a scientific programmer–this was many years ago. Actually, as it turns out, I am not a litigator but I think I am on pretty safe ground to say that mathematical theories would be admissible in court. A judge would probably take judicial notice of the science of mathematics, if you will, and bring in an expert to explain it all to him or her, because the odds are against his or her knowing it. And the court may even appoint a special consultant to advise the court–in other words, somebody not hired by either of the two parties, but somebody that the court would rely upon to help him or her. So, yes, there is no question–I think–that we're not far away from my ticket coming through first-class mail, to be honest. And I think I would pay it, rather than fight it. Okay? Next question, please. Thank you.

QUESTION: Good morning. I enjoyed your presentations, and was very interested by the concern you raised about the possible loss of privacy that would allegedly result from an increasing use of technology. But having lived for four years in the rural Middle East, I am quite aware that in a rural society there is absolutely no such thing as privacy. Everybody knows all your business, and they remember it. And–you know–it took me a while to calm down my paranoia, but it was interesting to put that, in turn, in relationship with the 19th Century French novelists that I study where, as Stendhal says, "There was never a police force better constituted than the women of a village, who know everybody's business and who remember it." And interestingly enough, for characters in 19th Century French Novels, the great fantasy is to come to America, where you have no known neighbors and no past. In those novels, you watch the characters develop subterfuges for avoiding surveillance–they're never very successful–but I am a little inspired by your notion of logging on to New York Times' website under cpunks. And I'm thinking of other methods of subterfuge because, as was pointed out last night, all of this requires our cooperation. I think maybe when I go shopping this afternoon I'll offer to swap shop cards so that he'll get my ads for whatever I buy and I'll get his ads for dog food. Do you envision that people would be willing enough, or eager enough, to protect their privacy that they would do something similar on the medical front? Like, if they were going to undergo some procedure like a root canal, you

know they'll just swap identities, for the afternoon, with a co-worker–assuming that the implications are probably not very grave.

PHYLLIS: Well, I think that is an interesting question, because the way employer-sponsored health plans are organized, it is dangerous to swap identities, even for the most mundane procedure like root canals, because you don't have any way to know about the medical expenses that that real person would have incurred. It may be that the effect of swapping identities is that your treatment would be rejected as being paid by the health plan. I can tell you, however, what I do see. I see people not submitting bills to their insurance companies or their employers for certain kinds of medical treatment, such as mental health benefits and some types of lab work. I see people willing to pay for those out of pocket, rather than going through the insurance they have because they are terrified that their employer will eventually find out about their medical condition. And I think that is a bigger danger, that more and more Americans, if they are afraid that this medical information isn't going to be protected, that they will become less likely to use the insurance and then that creates bigger problems. I do want to comment on your first comment, though, about the fact that it isn't just in cyberspace in which there is a problem about the ease of accessing confidential medical information, because people do know everybody else's business. That is really one of the reasons that is has been very hard to come up with privacy regulation. There is always going to be someone who knows something personal about you. There is no way to protect complete anonymity in this area.

CHRIS: I really liked your comment, especially the observation that in older cultures you have almost no privacy. And this is one of the nice things about America and cities, is you move to a society where you have the ability to say, "You know, I don't like the way my culture in this town uses me, so I'm going to pick up and I'm going to start a new life. And I'm going to move to Texas and start a new life. And maybe I'll escape my criminal record and I can go be an upstanding citizen." Well with the creation of more and more government and commercial databases, that is becoming impossible. And it is to the point now where

your commercial–your credit record–will have your arrest record on it. So, just creating the databases, in itself, creates a new form of social control that exists in older societies and are now being imposed on our newer societies. I would also say that a good way of privacy self-defense is to provide fake information and you made references to Sam Beckett, so I'll make references to James Joyce and, that is, I'm Buck Mulligan on my giant card, and they are never going to figure out who I am.

ANN: What is interesting about this new mechanism for data collection–all the supermarkets and everybody using these little "member" cards–what is interesting about this is if you actually read the waiver statement that you sign, you are not just agreeing to let them send you coupons. You are agreeing to let them sell your information for other things. And I know when I filled out my "member" card for a supermarket I refused to authorize this. And the person who was there at the counter said, "Well don't you want to get these discount coupons?" And I said, "It's not worth ten cents off on my product so that you can sell my name to everybody in creation and know what I am buying in the supermarket." So be careful, even of those commercial ones.

CHRIS: I'm sorry, I will be really quick. There is a California case where there was a slip and fall. Someone had a Von's Supermarket card and it turns out that this person bought a lot of beer. And Von's Supermarket sought to introduce the evidence that he was an alcoholic. So these things can come back to you.

PHYLLIS: I just want to interject; too, the point that you raised about people swapping identities for privacy is an interesting one. It does all ready happen when people use each others insurance cards because they don't have insurance, and in fact, the insurance companies are eager to see that be a crime. So it wouldn't just be a matter of the risk that you take because they believe different things about you, but in fact, swapping identities is fraud and subject to criminal penalties. And I actually suspect that if we do get any privacy legislation, that some of the entities, like The New York Times, will be eager to see that providing false information–using the cpunks thing–is criminalized. That that may be a *quid pro quo* for them

agreeing to any kind of privacy legislation. They will agree to privacy if you agree that you won't provide false information.

GARY: I think we have got time for one more question.

QUESTION: I appreciated your presentation. It was very informative. I am a student here, a master student, and I just started my own website. And I have a question now–you've got me kind of scared–I did not create my website, my partner who lives in Finland did. We have a commercial vendor who is hosting our website. I know he uses cookies: is there an easy way that I can figure out what cookies they are using, and exactly what my website is doing, and see if I can figure out how to bring myself into compliance with the fair privacy issues? And another question I also wonder is, my target people are prime candidates for research. Now, if I allow them to be studied on the aggregate by researchers, how do I address the privacy issue in that respect, too?

GARY: Before somebody–I just want to clarify your question: you have a website–and is it a link over to a commercial organization?

QUESTION: Actually, it is a market maker website. It matches people with broken cars to car-parts sellers and mechanics.

GARY: But do you provide a link, or is that what your website does?

QUESTION: The website just matches the people up. We don't do any product selling.

ANN: Yeah, I would suggest that you start with the entity hosting your website, and demand from them an accounting of exactly what they are doing. And once you know that, you can take a look at what the FTC suggests in terms of fair information practices, and just–you know–do a matching and see what it is you are doing. I think you need an understanding of what information is being collected, and then you can make decisions. If you do want to be protective of privacy, you can let your users know what you are doing and give them a chance to opt-in or opt-out. There

are going to be consequences for you, in terms of the data you collect and the accuracy of the data–you just have to make some calls. I am encouraged that you asked that question, though. I think that is great.

GARY: Actually that is an important question. In fact, it is going to force me to say one more thing before I let you go. I draft a lot of privacy policies for clients. And I am convinced the hardest piece of the privacy policy is for the person doing the drafting–sometimes a lawyer, sometimes a businessman–to really figure out what the technical people are doing. We have a real big gap between what information is being collected from a technical perspective, and what is being said in the privacy policy. And I think it was Ann who talked a little bit about–the worst thing you can do is have a policy out there and then not follow it, because now there is a problem, or at least a discrepancy, between what you are saying and the way you are doing business. Remember the FTC is now going to focus on the deceptive side of the equation. And if you don't know what the technical people are doing, in terms of collecting or even the ability to collect, you are not going to be able to draft a policy correctly. And I think that is why Ann's answer was very important to the last question. Before you do anything –before you figure out where to go and how to do it–you need to first determine what is going on from a technical perspective. Okay, I think we are out of time. Time to move on to the next program. I would like to thank the speakers and thank you. You have been a great audience.