ASSOCIATION OF AMERICAN LAW SCHOOLS 2001 ANNUAL MEETING: SECTION ON LAW AND COMPUTERS

JANUARY 5, 2001—SAN FRANCISCO, CALIFORNIA

PRIVACY AND E-COMMERCE

Jessica Litman[*]

MICHAEL MEURER:

I think we will move on to our next speaker, Jessica Litman. Jessica is a professor at Wayne State University. She is an expert on computers and the law and intellectual property law, with scads of important publications, including a casebook or a treatise on trademark law and unfair competition. She has taught at the University of Michigan and New York University law schools. Jessica will be speaking about privacy.

JESSICA LITMAN:

If you spent any part of the last two weeks reading those roundup articles they have in the newspapers about the year in e-commerce, you saw the same theme echoed again and again: "Where is the business model that makes money?" We do not seem to have found it. Subscriptions, when you are talking about selling content, have so far failed for works of general interest. Banner ads seemed for a while to be an obvious solution, but it turns out that consumers do not click on banner ads very often. Most people have figured out how to ignore them. What seems right now to look like it is going to be the most viable model is the delivery of "eyeballs" to merchants along with detailed demographic and other information. Targeted advertising follows this model. If you subscribe to the *New York Times* on the Web, you know it gives out free subscriptions in return for your answers to a slew of very intrusive questions. The *Times* uses that information to decide what banner ads go to whose eyeballs. The theory here is if you show me an ad for something I want

[*] Professor of Law, Wayne State University.

to buy, I will click through; and if you compile enough information about me, you will know what I want to buy. This is an information barter system. Content suppliers make content available at no cost in return for information about the reader, which is then sold to people who want to reach the reader.

The rapacious collection, sale, and rental of consumer information has completely transformed the bricks-and-mortar marketplace. Once upon a time, the stuff we think of as advertising was about delivering product to consumers. With the advent of targeted marketing, the paradigm has shifted. Advertising is about delivering eyeballs to merchants, and we are now the product.

What makes the Internet information barter system different from conventional bricks-and-mortar targeted marketing is that, in addition to compiling information that people are willing to volunteer (and people are willing to volunteer a *lot)*, when we do this on the Web, sites are able to collect information that people might not willingly volunteer, and to do so surreptitiously. Web sites collect click-stream data that can contain information about just about everything most people see. At least for now, that information is perceived as valuable. On top of that, sites can offer software applications for free download. The software applications can do nifty things. They also phone home periodically. They can tell their moms what computer programs and music files are sitting on consumers' hard disks and how often those consumers use and listen to them.

(Last year I lived in a dorm for four months, and for the first time connected to the Internet through a university network. So I downloaded and installed a personal firewall for the first time. And, boy, I was amazed at how many programs on my hard disk called their mother without telling me first. It was astonishing, and I like to think of myself as a cynical and suspicious woman.)

In any event, you get all this data. You can combine it with data collected offline, with addresses, with credit ratings, with Shoppers Advantage purchases, and with catalog orders. You can learn quite a bit about the eyeballs that you are selling, and the eyeballs that you are buying. Computers can now do all the correlating, slicing, dicing, monitoring and serving.

In the long-term, I think that the value of that information is, at best, unproved. Quite a few Internet service providers showed up in the last two years offering free access (and, indeed, free computers) to people in return for detailed demographic information and the promise to read the targeted ads that showed up on the screen. Most of those concerns have gone under. So long as the information is perceived as valuable, though, people are collecting it, slicing it, dicing it, and offering it for sale. There are companies who believe that they can predict your behavior based on the profiles that they generate from all these data points. Now, they may be right about this, or they may be wrong. Right now it does not matter because, so long as there are plenty of businesses willing to buy those profiles (because they *might* be able to do what they say they can do), the information is generated, it is collected, it is catalogued, and so forth. As long as people are willing to buy it, it is going to be perceived as valuable.

Think about Napster. Napster does not collect information, although it could. It has forty-four million users and it could collect all sorts of information about them. It has sort of promised that some day it will. It does not charge for its software services and it could. But it is unlikely that people would be willing to pay a great deal for Napster software and services simply because there are other programs out there with similar functionality that are going to be competing with it. Napster attracted fifteen million dollars in venture capital with no assets but a pending patent application and, at the time, about fifteen million pairs of eyeballs or, more precisely, ears. That is about $500,000 per ear. Napster's most valuable asset, then and now, is its installed base of customers. The subscribers are music enthusiasts; it is easy to keep track of what they like. That possibility attracted a great deal of money to a business even though it faced massive liability from copyright owners.[1]

Now, all this stuff is more or less invisible to the casual Internet user. It is not difficult to figure out what is going on if you pay careful attention, but most people do not. Some people find it chilling when they do an Altavista search for cancer and get back a banner ad for Procrit. Other people think, "Oh, gee, that's kind of neat. My computer *knows* me."

My students tend to argue that all of this is okay, so long as nobody can correlate the data collected about them online with the offline data collected about them in their real world transactions—so long as all this information has no real impact on their lives in the bricks-and-mortar world. But, of course, that data are already being combined. There are businesses out there who are linking your Web profile with your address (so that local merchants can buy ads on the Web to people who are within their area of service). There are businesses linking your credit history with your online identity (so that online banks can pull up your credit rating as soon as you submit an application for an online loan, and they can figure out whether or not they want you as a customer).

The *Yahoo!* case,[2] the *iCraveTV* case,[3] and the other cases that seek to require ISPs to bear some responsibility for giving access to content to people in different geographic areas, are only going to make this worse. If an ISP *has* to know where you are, then that kind of linking is going to become even more common.

The United States government has, for the most part, been supremely uninterested in regulating any of this. Why? I think it is a religious thing. Ten years ago, the Cold War ended. The United States declared victory and insisted that capitalism had proved its superiority to communism, socialism, or

---

[1] *See* A&M Records v. Napster, 114 F. Supp. 2d 896 (C.D. Cal. 2000), *aff'd in part, rev'd in part*, 239 F.3d 1004 (9th Cir. 2001).

[2] *See* La Ligue Contra Le Racisme et L'Antisemitisme v. Yahoo! Inc (Superior Court of Paris Nov. 20, 2000); Yahoo! Inc. v. La Ligue Contra Le Racisme et L'Antisemitisme, No. C00-21275 (N.D. Ca. filed Dec. 21, 2000).

[3] *See* Twentieth Century Fox v. iCraveTV, 53 U.S.P.Q.2D (BNA) 1831 (W.D. Pa. 2000).

any other economic or political alternative. It persuaded all of its trading partners to try a little dose of capitalism, so far with mixed results.

With no monolithic antagonist to battle, the United States has gradually invested in a version of neocapitalism that is exaggerated to the point of self-parody. We make a fetish of markets, especially the stock market. Coming up with a product, *any* product, the people are willing to buy has become a patriotic act. It fuels the economy, it raises the Dow Jones, it puts people to work. From that point of view, the folks who are trying to argue that one should not be able to collect that valuable, salable data, correlate it, and sell it to the highest bidder are not civil libertarians but out-of-touch old-timers whose obsolete ideas threaten to bring America down.

That whole ethos may be the explanation for one of the scarier suggestions out there for how to solve this problem. This is privacy protection in the neo-capitalist mode. The idea here is we should give people property rights in information about them, and allow them to license other people to collect, correlate, rent, or sell that information, thereby empowering them to control downstream use of their personal data. If you were at the *Defamation and Privacy* section, you heard this idea discussed in more detail than I have time to give it, but the sense is that even if this does not actually empower people, it will ensure that they are compensated for the value of their information rather than allowing the data aggregators to appropriate the value for themselves. And the idea has been endorsed by folks all across the political spectrum, ranging from left to right, all the way from Larry Lessig[4] on the left to Representative Chris Cox[5] on the right.

Now why do I think it is scary if it is so popular? I am one of those out-of-touch old-timers who wants to bring America down. I care about data privacy and, from that vantage point, I think that propertizing personal information is not going to empower anyone. Indeed, I think it is going to make everything worse.

The idea that this is going to empower people is based on the notion that property rights allow one to control downstream uses in a way that contract does not—that you can control use of your property by people with whom you are not in privity. So a condition that Amazon.com may not share your demographic data with anyone except under these conditions would be a covenant running with the facts and would be binding not only on Amazon, but on anyone Amazon shares the information with.

Why has this not happened before? The argument goes like this: transaction costs to bargain with Amazon.com over the terms and conditions are too high.

---

[4] *See* Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56, 63-64 (1999).

[5] *See House Telecom Subcommittee Holds Hearing on Online Privacy*, TECH L.J., July 14, 1999, ¶ 14 <http://www.techlawjournal.com/privacy/19990713b.htm> (reporting that Rep. Chris Cox proposed establishing a property right in personal information at the House Telecommunications Subcommittee hearing on online privacy).

Now, though, we are supposed to have these intelligent automated agents who are going to be able to do all this bargaining for us much more cheaply. I think the premises of that argument are demonstrably false. The transaction costs to bargain now are not especially high. They would be pretty cheap if data collectors wanted to bargain over that, which they do not. Your credit card company, for example, could put a little check box on the form you have to fill out anyway, saying, "Check here to save one to five percent in charges or costs, in return for our selling everything we learn about you," or "Check here to pay twenty dollars of no processing fee in return for our not doing so." Very cheap. What is expensive is not individually bargaining over your preferences. It is treating data differently in individualized ways, either putting them in different databases or flagging them so they can go out here, but not go out there. Nothing in current technology is likely to solve that problem. So, collectors of information are not going to bargain with consumers over how to treat their data, not because bargaining is expensive but because treating data in individualized ways is too expensive.[6]

In addition, I do not think the money that consumers are likely to be able to collect is going to add up to any meaningful additional compensation. They get some amount of money now in return for the discounts or the lower prices that they get as part of the system whereby they supply personal information to a merchant who then sells it. Calling that information "property" is not going to change the numbers in that equation to any marked degree.

That is why I think it will not work. It is not why I think it is scary. Here is why I think it's scary. Property is alienable. That is the point. We give out property rights chiefly to encourage people to sell stuff. Now, I can do a whole song and dance about this, but those of you who teach intellectual property know what I mean. These property rights are incentives that encourage people to generate and distribute whatever it is. People do not need an incentive to generate personal information; it happens in spite of us. I would not think that businesses need any greater incentive to collect the stuff than they already seem to have. Economic theory tells us that property rights in the information will encourage them to collect it, slice it, dice it, and sell it, even more fervently than they currently do. As an old fogy, I think that is a bad thing.

In addition, by denominating something as property, we legitimize the whole business of trading it, renting it, and selling it. That is what property is for. If I am right about the first point, which is that consumers will not in fact gain appreciably greater control or be paid appreciably more money for the transfer of their personal information, we will have a new world where data miners will have a constitutionally protected right to sell the information that they manage to collect.[7] Moreover, the legitimacy takes the shame away. The one thing that has caused packagers and sellers of personal information to take

[6] *See* Jessica Litman, *Information Privacy/Information Property*, 52 Stan. L. Rev. 1283, 1297-99 (2000).

[7] *See id*. at 1295-96, 1299-1301.

a step back in the past two or three years has been public shame. When they have backed off and repackaged their privacy practices, it is largely because journalists or customers have said, "Shame on you, Real Networks, phoning home about what is on my hard disk." If we make the system legitimate, if we insist this is how it is supposed to work, then the shame card is gone, and right now it is the only one that seems to be working.