Canada-United States Law Journal

Volume 29 | Issue 1 Article 37

January 2003

Discussion Following the Remarks of Mr. Theofrastous and Ms. Lussenburg

Discussion

DISCUSSION FOLLOWING THE REMARKS OF MR. THEOFRASTOUS AND MS. LUSSENBURG

MR. CARMODY: We have covered a number of very interesting and diverse topics, but I see that Henry has the microphone again. No surprise there.

MR. KING: I am interested in the civil liberties aspect of this. I would like to have you comment on personnel records, records of people, the civil liberties aspect of this. It has historically been a matter of concern on how France has taken a very rigid view of this. Perhaps Ted could comment on this. I think it is a very important question and one that has far reaching implications.

MR. THEOFRASTOUS: On the U.S. side, there have been some industry specific legislative measures put in place that have been relatively effective. In healthcare, there is HIPPA, which in some ways it is relatively common sense, as you know, you cannot talk about a patient in front of a third party. You cannot openly share anymore of the information than you absolutely have to in order to comply with the request, even under law enforcement directive.

In the financial services end, the Gramm-Leach-Bliley Act included some substantial improvements on the privacy side in terms of investors and investments. Meanwhile, you know, the EU Privacy Directive which has been implemented at the national level. There are national registrars in place that protect private data along the lines of it being a human right. That has been interesting. Self-certification in the U.S. has really been dropped since the Bush Administration. There was a strong move by the FTC to regulate privacy, but certainly to be involved in setting best practices for dealing with private data. Again, with a change of regime, the FTC indicated this was not their top priority.

MS. LUSSENBURG: There are similar concerns in Canada. The concerns take on two flavors from where I am sitting. First of all, we have privacy legislation in Canada. One of the issues that we grapple with is that it is more cumbersome than U.S. privacy legislation.

Working for a multinational corporation, I face the conundrum that many international operations do, which is which standard do you adhere to? Typically, you have to adhere to the more onerous standards. So you may be at risk of having to impose the higher Canadian standard across the rest of your operations for a truly global network and infrastructure. That is a huge challenge, and without telling tales out of school, it is fair to say that other jurisdictions are not that receptive when a foreign country seeks to impose

their privacy regime on others. As an operational matter within AT&T, it is a non-starter, because we are a much smaller part of the overall operation.

The Canadian Bar Association has put out a position paper on the Lawful Access Legislation that is being proposed in Canada. I will say it is a Lawful Access. It is really a consultation paper. There is no legislation yet. One of the biggest criticisms is that it is extremely weak, because it does not provide us with adequate detail to assess all the ramifications of what is being proposed by the government.

In their discussions, the Canadian Bar Association, they too have criticized the lack of concern in the legislation for recognizing personal privacy. They have questioned it from both a Constitutional perspective as well as a civil rights perspective, and have gone into an analysis as to whether or not there is the authority, the residual authority under the Peace, Order, and Good Government.

Again, for Canadians that will be very familiar, the residual power accorded to the Canadian Government to regulate in this area and then they have also raised concerns about the Charter and what level of privacy is one entitled to. In some respects one can scale that when you get to an industry standard where it is understood and acknowledged that you will have no privacy in these communications, but that leaves us open to a radically different society than one today. We presume that when we send a communication, and as lawyers we say they are privileged and confidential communications in rendering advice over the Internet or by e-mail, what does that mean?

MR. THEOFRASTOUS: I would add to that. Certainly in the workplace, from an employment law perspective, the standard line is more and more becoming you do not have an expectation of privacy for anything that you are communicating inside of the corporate network. This was initially a gray area. Obviously, there is still corporate responsibility with employment records, but in terms of the individual, forget about it. If you are writing a distress letter to your ex-wife on company time, the Personnel Manager may, in fact, be able to read that.

MS. LUSSENBURG: However, certainly under Canadian law, the position is that you must clearly communicate that position to your employees. Even then it is still not free from doubt, because if you pick up the phone and have a personal conversation, are you entitled to privacy in that personal conversation even though you are using your employer's equipment? Most people think they are entitled to privacy.

MR. McINNES: Simon McInnes, from Industry Canada. Selma, you mentioned something very briefly about foreign ownership restrictions on transmissions and then you switched topics. I wondered if you could expand a little bit on what you were referring to.

MS. LUSSENBURG: Sure, happy to. It relates in part to what is in the Lawful Access Paper. I do not think I have a copy right in front of me, but as you know, the ownership of transmission facilities under the Communications Act in Canada is subject to foreign ownership restrictions. The test is 50 percent equity, 33 percent of voting control. Those are the maximum thresholds allowed through the infamous Unitel case, which was a company AT&T had a significant investment in until two weeks ago. The ownership of transmission equipment being restricted to Canadian Nationals, when you look at it from a multinational perspective, it is obvious that there are similar restrictions in other jurisdictions. When you start looking at applying a global standard it makes it far more difficult, because you have one Canadian standard and you have a different standard internationally. So, you do not always control the services.

For example, we are deploying a whole new network in Canada. It is a leased line network. We buy our services from the incumbents. Therefore, we would need to insure that the incumbents were compliant, and one would hope that they would be. It is a whole new level of layering in the industry. I am not suggesting foreign ownership is a new issue in Canada. It has been around for a long time, but it adds an additional burden upon the telecommunications service provider. In particular, when we translate the issue into practical terms, Internet service providers, many Internet service providers are foreign owned in Canada.

MR. GELFAND: Marty Gelfand. I have a lot of distrust for telecommunications legislation. The 1996 Act made things less competitive. Large radio companies are gobbling up small radio companies all over and we end up with less variety along the radio spectrum; issues that I think hinge on antitrust problems although they may not have been defined that way. I have concern about more legislation on the Internet. I enjoy a small Internet service right now, where I do not get barraged with spam. I do not have to put a footer on my e-mails advertising my Internet provider. I do not pay a lot of money per month. It is a pretty decent Internet service.

I am concerned that legislation is going to change that when the Yahoo's and the AOL's gobble up the small Internet providers that I personally enjoy using. Again, this would hinge on antitrust with probably some anti-antitrust loopholes thrown in.

MS. LUSSENBURG: I think you are right. It is one of the issues that the industry has pointed out is that there is, as you impose additional controls there is a significant cost associated with it and the less the likelihood will be, depending on the level of change required in the industry to accommodate, monitoring the Internet and data preservation and data retention. If the cost burden is high, the small players will go out of business. We have that problem in the Canadian market, and we are not even talking about

regulating small Internet service providers. The telecommunications industry is extraordinarily capital intensive. They need a lot of money.

MR. THEOFRASTOUS: I would add that the 1996 Act also promises, at least for the small guy, that if you were an Internet service provider and you wanted to become a telecom provider, you would be guaranteed a high level of cooperation from the larger providers. You were supposed to sort of be given a little bit of a leg up.

In reality, it just has not worked out that way. There have been a number of initiatives that failed. They failed because it was a capitally intense proposition, but also because they could not get the level of connectivity they want.

I can tell you that I recently tried to explore the regulatory side with a small ISP here in Ohio that wanted to go this route. The Public Utilities Commission in Ohio was fully willing to help, but their information was bad, their contracts were out of date, and the upstream provider would not return phone calls. It is not like you could then call the telecom police to go and make them comply with the 1996 Act.

MR. DULAY: I would like to add to Mr. Gelfand's comment. My name is Brendon Dulay. I think of Andy Warhol's comment. He said that in the future everyone will be famous for 15 minutes. I think if he were alive today after his botched appendectomy, he might be saying in the future, everyone's life will be private for about 15 minutes.

I would like to relate a personal experience as acting general counsel for a small tier one Internet provider about how private you may think your Internet communications are. Marty, you might want to start writing in a foreign language once you listen to this. I represented a tier one Internet service provider. Tier one is higher up on the food chain, tier two is lower, and then tier three is basically college graduates and CIF's who open up. Basically, a router in their apartment and then they are classified as a tier three ISP.

We were faced with a conspiracy amongst our employees who were angry at the President, my client. They were doing all sorts of things including a network outage and destroyed the network for about three days because they wanted to get revenge on him. They made the mistake of conducting their conspiracy by e-mail. They used the company's e-mail. After that, they thought they got a little more clever after a lot of them got fired. They decided to route it through our friend's tier three Internet provider. What they forgot was that the tier three internet provider, which was again essentially a college graduate's company located maybe in his coat closet, that they had a router in that apartment, happened to be co-located in our company's co-location cabinet downtown.

My client went to the co-location cabinet and just put a wire in there, and got all of their conspiratorial communications through the tier three

co-location cabinet. I never asked them to do this because I have a much stronger view of privacy than my clients did, they present me with a very thick sheaf of printouts of exactly what they thought of my particular client, who by the way was gay, and they did not like that. They had the plans for their conspiracy, what they were going to do, and when they were going to do it. Basically, they had everything except the network outage. There it was.

The two guys had the audacity to file an employment lawsuit against my clients. They did not realize what would happen when my client would go into Court with big sheafs of documents showing exactly what they typed in to each other. Suffice it to say, that they were crushed. They did have an expectation of privacy, and they were working in the telecommunications industry. It did not work out too well for them in Court. I thought my client would be received in Court by the Judge as the technological equivalent of a Peeping Tom. However, the Judge did not look at it that way. Instead he said you are running a company and it is your equipment, your computers, and you happen to intercept all this traffic, concluded by saying, "Then all we are doing is accessing the truth. We are supposed to be afraid of the truth as lawyers? There are no real privileges here." All the stuff came in without any problems.

I think this type of behavior is going to grow more than it is going to shrink. I just wonder if there is a point where the Telco's themselves almost as a matter internal corporate ethics should say to national states and international law enforcement bodies, "Hold it. You are not going to look into a person's records."

MR. THEOFRASTOUS: I think there have been some efforts by industry to dig their heels in when they thought they could; in a particular to protect anonymity. I am sure you are aware in the cyber-smear lawsuits where a person makes an anonymous posting on a bulletin board. The major cases have been either something that sounded like insider trading or even just disparaging remarks about an individual. Yahoo says, "No, I will not provide that information." But the District Court says, "Oh, yes, you will." Ultimately, the threshold seems fairly low to me. My question is to the extent they do dig in, if you do not have the political will to acknowledge that, whether it would have an effect?

MS. LUSSENBURG: I find your story fascinating and entertaining. I have a couple of observations. One is certainly as a corporate policy, we do not monitor our employees' e-mail. The only time we look at e-mail is when there is an issue. For example, we got complaints not too long ago of pornographic material being distributed and when someone was being harassed. At that point in time we felt when we approached the employee and they continued to deny that they had anything to do with it and we knew the identification, where it came from, and that we had to go back and check in order to confirm the basis for which there was disciplinary action.

As a company, we have a corporate policy that while we tell our employees that the Internet communication is not private and that you are using company resources, we do not scan or look at Internet communications. It is contrary to our corporate philosophy. I also think that you have to distinguish when you look at your situation whether or not as an ISP you are providing information to a third party under lawful process, or whether or not you are actually just giving that information because someone calls you.

I can only speak to our experience, which is that the rules are the same in Canada and the United States. As a company we only release information after there has been a warrant or other similar document been issued by a Court of competent jurisdiction. We force the U.S. authorities to go to the Canadian authorities to get their warrant authorized. We will not just release information even though at first blush it may seem wholly reasonable, but you have an obligation of privacy to your customers. If you look at an ISP contract, it will say that the information may be released under lawful process. You have to give yourself that protection. You have a lawful process defense for the disclosure of somebody's private information.

MR. CARMODY: I think we have time for just one last question.

MR. SHANKER: Morris Shanker. Selma, you touched on something that I have seen throughout my practicing career. The rules and regulations and decisions are usually made by lawyers. They are often regulating highly technical matters of which they have no background and little understanding.

If they pass statutes like the one you mentioned, where it is illegal to receive a certain kind of e-mail, what do you do about the breakdown in communication? How do you educate those who sometimes do not want to be educated? The lawyers who are really running the show, on highly technical matters for which they do not understand? Do you have any comments on the problem and if there is any possible solution to it?

MS. LUSSENBURG: We have talked about this a number of times and the Canadian ethos is very different from the American ethos. We lobby our government far less than Americans do. Part of it is setting up meaningful communication with those people that draft the legislation. That means the business community has to allocate the time and resources to engage in the dialogue. Sometimes business is not prepared to allocate those resources.

AT&T has a group that is working on data retention on a worldwide basis because we see it as a very big issue for us if the legislation comes in and it is too broadly applied throughout our global operations. But on a day-to-day basis within our operations, I am the only one that is familiar with the issue in Canada. I do not spend my time lobbying the Canadian Government, because I just do not have the time.

We do have industry associations. The Information Technology Association has put out a very good position paper on the issues. The

Canadian Bar Association (CBA) has prepared a far more, not surprisingly, legalistic position on it. When I read the CBA paper, I thought these guys were on the right track, but they do not understand how telecommunications works, right? I think it is a huge, huge problem. I think the industry, in part, has to get out there. Oh, he has left. I was going to say, with deference to Industry Canada, you know, hit them over the head with the information. Having said that, there are many very good industry working groups.

MR. THEOFRASTOUS: On the U.S. side, I think there is a growing tendency to install advisory committees and advisory councils at fairly high levels. There is an advisory council specifically on the IT infrastructure to the President. It has heavy hitters on it and good industry representation.

What makes me a little uncomfortable with that is that you have got people like Bill Gates on the Council. Bill Gates is a great, smart guy, and I am sure he will devote some modicum of his time to actually trying to produce an outcome. But once it becomes a parade of the rich and famous rather than the smartest minds you can find to try to address the issues, I think the outcomes are potentially not as good as I might have hoped for.

MR. CARMODY: When I undertook to chair this session, I was informed that one of our speakers has a skating recital that she must attend in Mississauga this evening. So, we do have to end exactly here. I want to thank both of these presenters. They were extremely informative. And thank you for all of your questions.