Canada-United States Law Journal

Volume 29 | Issue 1 Article 36

January 2003

Security and the Economy: The North American Computer and Communication Infrastructure - Canadian Speaker

Selma M. Lussenburg

SECURITY AND THE ECONOMY: THE NORTH AMERICAN COMPUTER AND COMMUNICATION INFRASTRUCTURE

Selma M. Lussenburg[†]
Canadian Speaker

My presentation falls very well onto Theo's presentation. One of the reasons we wanted him to speak first is that he has given you a perspective of what the Internet and telecommunications look like. I want to speak to some of the more nitty, gritty legal issues that come out of it and the economic concerns the telecommunications industry has. When I speak about the telecommunications industry, I think it is fair to say that my views represent a consensus. I work for the American AT&T Corp, which is expanding slowly but surely globally. We are building a new network throughout the world to support our global customers, particularly multinational corporations. As we look at cyber terrorism and we look at security in the context of the telecommunications industry, there are some significant hurdles, as you can tell by the graphic depiction of what a network looks like and what an Internet Service Provider's (ISP) network would be.

The industry has been working on a position paper. This includes the International Chamber of Commerce, the International Telecommunications User Group, the Union of Industrial and Employers Confederations of Europe, as well as the largest Internet service provider group in Europe, not to mention we also have in Canada the Information Technology Association, and other similar groups. There is tremendous concern about balancing the need to modernize legislation with what is technologically feasible, and the

---

[†] Selma M. Lussenburg is Chief Regional Counsel for Canada and Vice President, Legal Affairs and General Counsel for AT&T's Canadian operations, a position she has held since 1998. She joined AT&T Canada Enterprises Company as Corporate Counsel in 1997. Prior to joining AT&T, Ms. Lussenburg practiced with the Toronto law firms of Borden & Elliott, Fasken Martineau DuMoulin, and the Sydney office of the Australian law firm of Allend, Arthur, Robinson. Ms. Lussenburg is a Canadian representative to the Trade Ministers' NAFTA Advisory Committee on the Resolution of Private International Commercial Disputes. She is also a member of the Advisory Board of the Canada-United States Law Institute. Ms. Lussenburg received a Certificate of Private and Public International Law from the Hague Academy of International Law in The Netherlands, an LL.M. from the Australian National University in Canberra, Australia, a graduate level Diploma in International Co-operation and Development from the Institute for International Development and Co-operation, as well as LL.B., *cum laude*, and B.S. degrees from the University of Ottawa.

cost associated with putting in place a legal network, if you will, or a legal regime that is transparent and realistic. When you look at that example Theo showed us, the video that we saw, and they are flying under the radar screen, I do not know how you combat that. I do not think there is any technology or software that you can put in place to deal with that; absent totally slowing down traffic in the telecommunications industry.

I propose to look at the Council of Europe Convention on Cybercrime,[1] which is very similar to some of the provisions found in the U.S. Communications Assistance for Law Reform Act in the U.S. There is a discussion paper put out by the Canadian Government called Lawful Access.[2] They raise a number of common issues and concerns. First, though, I want to reiterate the obvious. We heard Mr. Flynn speak passionately yesterday about the need for balance, transparency, and accountability. We also hear people talking about the need for a common border, common security measures. Telecommunications services are like much of Canada-U.S. trade, the highest volume is across the Canada-U.S. border. There are more telephone calls between Canada and the United States, and there is more data exchanged between Canada and the United States than anywhere else in the world. So it is a laudable objective if you think you can close off the North American perimeter for telecommunications. By its very nature, telecommunications knows no boundaries.[3]

When you send an email to your mother from Toronto to Vancouver that e-mail message may well go to Singapore before it actually comes to Vancouver. There is this traditional view that when you call someone, it is a linear transaction or linear communication. For those of you that were Canadian, or are Canadian, you may remember the Ward Air commercials where they would advertise that you wanted to go from Toronto to Chicago, but your luggage would go to South Africa before it would reach you and that is how you could travel internationally. Your telephone call is like that. Many, if not most, calls are international in nature; even when you are calling domestically within the North American marketplace because of the need to route traffic most efficiently.[4]

The other point I want to make as a general principle is that Canada has foreign ownership restrictions.[5] There are many other countries that have

---

[1] *See,* Convention on Cybercrime, Nov. 23, 2001, art. 2, EUROP. T.S. No. 185, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[2] DEPARTMENT OF JUSTICE CANADA, LAWFUL ACCESS – CONSULTATION DOCUMENT, Aug. 25, 2002, *available at* www.canada.justice.gc.ca/en/cons/la_al/law_access.pdf

[3] Michael J. Madison, *Rights of Access and the Shape of the Internet*, 44 B.C. L. REV. 506 (2003).

[4] Rob Frieden, *Regulatory Opportunism in Telecommunications: The Unlevel Competitive Playing Field*, 10 COMMLAW CONSPECTUS 98 (2001).

[5] Telecommunications Act, S.C. 1993, c. 38; Canadian Telecommunications Common

foreign ownership restrictions either on the ownership of transmission facilities or on who and how you can operate telecommunications facilities. We have no international standard to deal with all of these issues. When we start looking at telecommunications services, and you want to have an effective control mechanism to deal with crime, you are really looking at trying to build an international consensus. Because, otherwise, what you are looking at for a global telecommunications service provider is that you must meet all standards. This is what we are grappling with. We provide global roaming through our own facilities in 70 countries in the world and through third party service providers through another 80 or 90. We are forced to come down to the lowest common denominator once we move beyond the networks that we actually can control.

So what does the convention call for and what does the Canadian Access Paper call for? They call for the criminalization of certain offenses relating to computers, the adoption of procedural powers to investigate and prosecute cybercrime, and also for the promotion of international cooperation. They all seek to combat terrorism, drug trafficking, price fixing, money laundering, smuggling, Internet and telemarketing fraud, and the distribution of child pornography. All of those are obviously highly desirable policy objectives.

In Canada, under the traditional legislation that exists today, under the Criminal Code and under the Canadian Security Intelligence Act and Competition Act many of the offenses and procedures already exist,[6] but there are changes required to production orders, preservation orders, and it is being proposed that there be an offense in relation to the propagation of computer viruses. The current discussion paper proposes that it would be an offense to receive a virus on your computer. I think you can imagine why the industry is up in arms. It is not something that one can control. And you, yourself, as the consumer, cannot control this. While the public policy objectives are laudable, the concern is that we need to balance those against what is actually possible given the nature of telecommunications.

Looking at three of the main areas affected and why they are concerns in terms of the need to update outdated legislation. First, we will look at wire line, which is your traditional telephone communication by voice. We have for years had cooperation between the telecommunication service providers

---

Carrier Ownership and Control Regulations, SOR/94-667 (Oct. 1994) *available at* http://laws.justice.gc.ca/en/T-3.4/SOR-94-667/text.html; *Also see*, Barbara Miller, *Foreign Ownership in Canadian Telecommunications: Can an Explosion be Regulated?*, FASKEN MARTINEAU DUMOULIN, LLP (2000), *available at* www.fasken.com/web/fmdwebsite.nsf/0/AC520936FE629A77872569D8005F8D61/$File/FOREIGNOWNERSHIP.PDF?OpenElement

[6] Canadian Security Intelligence Act and Competition Act, R.S. 1985, c. C-23, *available at* http://laws.justice.gc.ca/en/C-23/text.html; *Also see*, Gordon Scott Campbell, *Emerging Issues of the Internet and Canadian Criminal Law*, 3 CAN. CRIM. L. REV. 101 (1998).

and law enforcement agencies. It is, however, the introduction of those services that we all love, call forwarding, data storage, and data retrieval that have created new obstacles because of the technology associated with them and the ability for law enforcement agencies to get access to that data.

In the wireless field, the expansion of wireless communication tools including cell phones, wireless e-mail, Internet devices, and satellite communications pose significant challenges for law enforcement agencies because they now have to deal with a variety of companies and a diversified combination of network infrastructures. I can assure you that Theo's diagram is not an exaggeration. If anything, it minimizes the complexity of how you get that telephone call. The Internet is a complex web, and there is no centralized control over the Internet.[7]

I do not want to spend too much looking at the Canadian legislation, because I think there are a number of interesting issues that have come out of the various pieces of proposed legislation. One of the issues that is out there is the ability to provide for basic intercept capability on all new telecommunications equipment. Putting it in very plain language, I would say to you - think money. This means new software. This means new equipment.

It may be a boon for the computer industry, but that too will be at a tremendous expense for those who have to buy the hardware and the software. Typically, that is not just the telecommunications service provider; it is the customer, the consumer, the business that must put that equipment on site in their router in order to provide that ability. It also provides an order to assist with exercising search warrants and authorizations that all telecommunications associated data must be stored. I would like to come back to that, but my first question would be what is telecommunications data? There has been a tremendous trend to give that a very broad interpretation. Secondly, it is not only what is the data, but how long do you preserve it? Do you preserve it on a continuing basis or on a prospective basis?

When we look at the issues, we are looking at the scope of the obligation, the costs, technological requirements, and the damage to end user confidence where we all presume when we are sending an e-mail. We presume there is a certain level of privacy afforded to that e-mail communication. The first issue is the excessively broad definition of traffic data. From an industry perspective, it is essential that governments narrowly and clearly define the traffic data types that are required to fight terrorism and crime and realize what is realistically achievable. Is that the traffic data that communication service providers routinely capture and retain for business purposes? If not,

---

[7] Lateef Mtima, *Trademarks, Copyrights, and the Internet*, SH085 ALI-ABA, at 390 (April 2003).

what additional information is truly needed and is useful for the purpose for which it is being sought? The Canadian definition, for example, is far broader than simple origin, destination, time, and duration of a transmission.

When we look at excessive storage periods one of the issues is the difference between data preservation versus data retention. Let me tell you what the difference is between the two. Data retention regimes require communication service providers to keep and store all records of preidentified data for an established and frequently lengthy period of time.[8] Data preservation, on the other hand, which is where the industry would like to go, requires data to be preserved after there has been a lawful request by a competent authority for information. It is based on the facts of a specific case.[9] Specific historical data can actually be preserved to prevent its deletion pending an issuance of a further demand for the additional information required.

The Canadian Government appears to be moving towards data preservation as opposed to data retention. But there are, particularly in Europe, proposals ranging from three months to three years for data retention regimes.[10] That is a significant administrative burden being imposed on the communication service provider. Let me be clear, nothing that has been put out has suggested that the government would pay for any of these services. It is very clear from the U.S. legislation and the Canadian proposed legislation it is a user pay system. The telecommunications service providers will bear the largest burden. Hence, the need to define reasonable rules of the road that will achieve the desired objective of combating the crime at hand.

COSTS

Traffic data storage can result in massive costs. We have a team of people in AT&T, in our government policy group, that actually work on data retention issues. I do not purport to do it on a day-to-day basis. We talked about costs and this concept of retaining data. There are a couple of aspects to costs. It is not just keeping it. It is once you have got it, what do you do with it? How do you protect it so that the consumer's privacy, whether that is a business consumer or an individual, is maintained and honored in the process? When that request comes for data that is two years old, how do you locate it? How do you sort and filter it? And as someone said to me, do you

---

[8] *Data Retention for Regulatory Compliance*, at 4, CARTESIAN, (2003), *available at* www.cartesian.co.uk/pdf/Data_Retention_White_Paper.pdf

[9] *Id.*

[10] Directive on Privacy and Electronic Communications, 2002/58/EC (July 12, 2002) *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en 00370047.pdf

have the FBI roll up and there will be 15 dump trucks of information that is going to be turned over? How useful is that information? Where do you put in the tags that allow you to find the information in a user-friendly manner and in a meaningful manner?

These are all issues that have to be considered and developed. I would like to be clear that I do not think it is the industry's position that there should not be any of this. The question is how do we do it in a manner that makes sense? There has been very little consultation, generally speaking, with the industry.

When we look at the Canadian Government's Lawful Access Paper, as someone who is in the telecommunications industry, and those that know me well will tell you that I do not hold out my shingle as a Telco lawyer. I hold out my shingle as a general counsel with a very strong commercial practice. I know more about telecommunications than most of you do, but I am still not a Telco lawyer. As I read the Access Paper, it is patently obvious to me that those that wrote the paper know nothing about how networks talk to each other; absolutely nothing. That frightens me. It is great to have the principle, but the issue is finding a way to bring that down to a level that can actually be applied in a practical manner. As part of this initiative to data retention and data preservation, we took a look at all of our U.S. and AMEA-based business units. Just to give you a flavor of some of the different aspects of this we surveyed consumer Internet, business names, managed instant messaging, mail relay services, access control logs, registration logs, web server logs, configuration service logs and business Internet services, just to name a few. We tried to assess what our current practices were. They ranged from days to up to 52 weeks. The cost ranged from in the thousands to $50 million, depending on where the restriction is on a per anum basis. That is just to access the data, not to store it and not to develop the software to actually extrapolate the data in a meaningful manner. It is millions of dollars. When we look at the actual costs of Internet crime it is more like a $200 million exposure. If you are looking at a $50 to $100 million expenditure per anum to support it per Telco, you are looking at a significant investment that will have to be ultimately translated into a cost to the consumer.

TECHNOLOGICAL REQUIREMENTS

That leads me back to reasonable technological requirements. What is reasonable under the circumstances, what can actually be retained, and how do we retain that data? For example, some of the technological requirements are wholly unworkable; witness my example of requiring those or making those that receive a virus to be liable for the receipt of the virus. Not to be forgotten is the damage to public confidence when we start looking at the

many issues related to the preservation of data and tracking data within the Internet and the telecommunications services industry.

I focused on the Internet because I think we are all closest to that, but very little consideration has been given, for example, to carve-outs to measure business to business intranet activity.[11] We have a virtual private network within our corporation, as does GM, as does Ford, as do most of the banks. Where is the need? Where is the risk? Is it an external or is it an internal one? I do not have the answer for you, but I think in determining what is appropriate, one has to look to that.

Many unfamiliar with networks have suggested that backbone service providers must bear the burden of data retention and data preservation. However, the Internet backbone is ubiquitous and much of the data that is sought by law enforcement agencies is not available from backbone service providers. In fact, it would be available from Internet service providers. The Canadian Government has stepped away from regulating Internet service providers. One of the remarkable situations in Canada is that the CRTC, which is the Canadian equivalent of the FCC, has refused to take control or to regulate Internet service providers other than resellers. So, many of the rules that apply to Telco's do not apply to Internet service providers.[12]

I will tell you that the industry which I represent and that of Internet service providers is not putting up their hands and saying to the CRTC, "Oh, please regulate us." But it is when we start looking at where the challenges lie. There first has to be an assertion of jurisdiction. How does one properly assert that jurisdiction? I think I will leave it at that. That way we will have some time for questions. I thank you so much.

---

[11] *See generally*, Christopher V. Cotton, *Document Retention Programs for Electronic Records: Applying a Reasonableness Standard to the Electronic Era*, 24 J. CORP. L. 417 (1999).

[12] *Supra* note 5.