

January 2003

Security and Freedom: Are the Governments' Efforts to Deal with Terrorism Violative of Our Freedoms - Canadian Speaker

Michael Power

Follow this and additional works at: <http://scholarlycommons.law.case.edu/cuslj>

Recommended Citation

Michael Power, *Security and Freedom: Are the Governments' Efforts to Deal with Terrorism Violative of Our Freedoms - Canadian Speaker*, 29 Can.-U.S. L.J. 331 (2003)

Available at: <http://scholarlycommons.law.case.edu/cuslj/vol29/iss1/49>

This Speech is brought to you for free and open access by the Student Journals at Case Western Reserve University School of Law Scholarly Commons. It has been accepted for inclusion in Canada-United States Law Journal by an authorized administrator of Case Western Reserve University School of Law Scholarly Commons.

SECURITY AND FREEDOM: ARE THE GOVERNMENT'S
EFFORTS TO DEAL WITH TERRORISM
VIOLATIVE OF OUR FREEDOMS?

Michael Power[†]
Canadian Speaker

I want to turn your minds back to yesterday to when Mr. Steve Flynn was speaking. He had a very masterful presentation and one moment when we all laughed, he was telling you about the containers that came from, I believe it was Slovakia.

MR. FLYNN: Slovakia going to New Hampshire.

MR. POWER: Five containers got on the truck. Then he told us it took 12 hours to get from Montreal to -

MR. FLYNN: To Vermont.

MR. POWER: We then discovered the truck driver was in the red light district. Keep in mind, when you talk about freedom you are talking about security. You can look at it from a different perspective. In that particular story that Steve told was about tracking a box. What if you shifted perspectives. What if you shifted focus and it was about the truck driver and you forget about the box. When you talk about the technology that is available today, it is very easy to shift that perspective, depending upon what you want to do. In large part, that is the issue today.

FREEDOM INCLUDES PRIVACY

What I want to talk about is security and freedom. What I want to present to you today is the idea that freedom does include the concept of privacy. You can see from this bio here, I am from Canada and I am speaking from

[†] Michael Power is a partner at the Ottawa law office of Gowlings, Lafleur, & Henderson LLP, practicing in the areas of privacy, authentication, security, electronic government and Internet law. During his career with the federal government, Mr. Power provided legal and policy advice to the Department of Foreign Affairs and International Trade, Investment Canada, Industry Canada, the Department of Justice and Treasury Board of Canada Secretariat on matters pertaining to information technology, electronic commerce, trade and investment issues. He speaks extensively on privacy and security subjects and has spoken to audiences at events such as the annual meetings of the American Bar Association, the Canadian Bar Association, the American Society for Industrial Security, and the Canadian Information Technology Law Association. Mr. Power received an LL.B. and an M.B.A. from Dalhousie University.

the Canadian perspective. We have section seven in our Charter.¹ It is called the Charter of Rights and Treatment Document. I actually refer to it as more of the Action Rights Charter of Permissions of Freedoms and Permission, qualifying everything in the Charter. It is really not a right you get, but a right we can take it away.

There is this quote from a case that dealt with section seven and privacy. I thought the quote was presentable to you as an audience because in particular, when you talk about freedom you have to focus on the subject of privacy. A lot of people when they talk about freedom they think of physical freedom, freedom from imprisonment. What I want to present to you is that in today's society a large part of freedom is psychological and in part, depends upon the act being left alone.

One component of that is information privacy. My presentation tonight is to present to you some of the more interesting aspects of responding to September 11th and implementation of mechanisms in Canada. We are essentially building surveillance infrastructure. It has been built over the last couple years and continues to be built.

INFORMATION PRIVACY

When you talk about the kind of world we live in the 21st century, what you essentially have is a new kind of war. We have Al Queda. We have people trying to set off bombs on airplanes and people using airplanes as weapons. This new kind of war requires vigilance in the identification of threats. You heard the first speaker yesterday morning. He says we do not know where the threat is going to come from. We have to be ready for it.

In order to do that, you need comprehensive information. They use it to a certain extent today, but it will become more prevalent in the future because the software and the artificial intelligence is on the horizon. You are going to see the deployment of more and more predictive analysis of information to determine possible threats. The idea being that completely isolated random bits of facts can be correlated and tabulated to determine a possible threat. That will become more and more possible in the future with technology.

In order to do that, you have to have a very comprehensive collection of information. Technology today, when you think about that comprehensive collection of information, makes it more manageable. Then when you couple that with authority, you have the ability to create a surveillance infrastructure. In times of war, people in the street will say that is okay. I can live with that, because I have to make a sacrifice. Everybody has to make a

¹ Canadian Charter of Rights and Freedoms, Can. Const. (Constitution Act, 1982) pt. I.

sacrifice. If somebody intrudes on my personal freedom a little bit, that is okay. It is my bit for the war.

Temporary surveillance in that context is viewed as acceptable. However, I will suggest to you, permanent surveillance is not. The issue at the end of day is not that information is collected, because somebody pointed out to me an article saying privacy is dead. I often remark to my partner, Ron Dearing, when you talk about what is going on in our firm, we hear little tidbits here and there. I did not know there were any secrets. It is just a question of who knows and who does not know. That is the same for a law firm or society or any other organization you are in. It is a question of who knows and what they are doing with the information.

I would submit to you that the amount of information collected, the length it is held, and the purposes for which it is used becomes very important. In Canada we have an Anti-terrorism Act.² We have a Custom's Act and Amendments to the Custom's Act.³ We have a proposed Public Safety Act. We have a national identity card proposal, which we thank you Americans as we have to deal with something you have caused. We also have lawful access proposals. I will not talk about them to much.

Settlement today in the communications session went off on a tangent about lawful access proposals. I agreed with everything she said. It is another piece of what I would call the surveillance infrastructure that is being created. The Anti-Terrorism Act got war decent right after September 11th, when we decide to make a law in Canada.

The Anti-terrorism Act added some new crimes and amended our criminal procedure law to deal with the subject of terrorism and the new kinds of threats that are out there. What it did in the area of electronic surveillance was akin to what amendments had been made in the United States. If I try to interpret a little bit of post 9-11 data. You basically took the United States domestic surveillance legislative framework and roughly made it equivalent to your foreign intelligence surveillance framework.

In Canada, we roughly did the same sort of thing. We extended the validity of wire taps from 60 days up to a year when investigating a terrorist group. What a terrorist group is is anybody's guess. We added the power of preventative arrest. The right to remain silent has been eliminated. Individuals with information about terrorism can be presented to a judge and forced to answer the questions. You are obliged to do that and we will hit you with penalties and anything else afterwards. The right to be remain silent is a cornerstone of the common law that we have had for centuries and has gone out the window in the blink of an eye in response to 9-11. We amended the criminal code to criminalize on-line hate propaganda. What this has to do

² Anti-terrorism Act; S.C. 2001, c. 41, s. 83.01.

³ Canada Customs and Revenue Agency Act; Interpretation; S.C. 1999, c. 17.

with terrorism, I do not know, but we did it. We amended the Human Rights Act so that the idea that hate messages by telephonic communications included all telecommunications technology. Anybody remember the case of Ernst Zundel?⁴ I mean these two amendments were to deal with the inadequacies of law in drying to deal with Ernst Zundel's situation.⁵ It was not anything to do with terrorism, but the act came along and we did it. It amended our private sector privacy legislation, prohibiting the disclosure of information under access request legislation. That was a little bit of housekeeping stuff.

The CSE is the Communication Security Establishment. It is our equivalent of the National Security Agency (NSA). Prior to the Anti-Terrorism Act, the only public reference to CSE was one page in the national archives basically a document establishing it.⁶ It is an arm of our Department of National Defense. You heard a lot of talk today about what Canada does in terms of its military and you heard the stories about our seeking helicopters. One thing that we are exceedingly good at is military intelligence and the collection of information. The CSE is the primary vehicle for that in Canada.

I have this segway into the CSE, because right in the heart of the Anti-Terrorism Act is this amendment to the Department of National Defense Act laying out a whole section describing the powers, the privileges, and the rights.⁷ This is sort of your basic departmental housekeeping legislation, but how come it is in the middle of the Anti-terrorism Act? I actually asked this to the members of CSE. I said you really had this in the can, you know, you really had this ready to come out when the moment occurred? He looked at me, then began swearing. What I am getting at here is that the Anti-Terrorism Act seems to be an opportunity to use September 11th as an excuse to do some things that people wanted to do.

Those in Canada will be familiar with the advanced passenger information and personal name recorder data base that requires 34-pieces of information. This is an amendment to the Custom's Act, whose stated purpose is risk evaluation. So when you are coming to Canada, we get some

⁴ Marlene Habib, *Group seeks 'swift removal' of Zundel*, HAMILTON SPECTATOR, March 7, 2003, at B5, available at 2003 WL 14600220

⁵ *R. c. Zundel*; 1992 CarswellOnt 995; Cour Suprême du Canada; August 27, 1992; Docket: 21811.

⁶ Established in 1946 as the Communications Branch of the National Research Council, the CSE was transferred to the Department of National Defense in 1975. *The Communications Security Establishment and the National Cryptologic Program*, Fact Sheet, COMMUNICATIONS SECURITY ESTABLISHMENT, available at www.cseccst.gc.ca/en/about_cse/about_cse.html

⁷ National Defence Act; R.S.C. 1985, c. N-5

information on you in advance so that we can screen you and focus on you as opposed to somebody else like me, for example.

What I found interesting is that when you look at section 107 of the Custom's Act, Paragraph O, you go from A to O. Customs CCRA can disclose the information that they collect and they got a list from A to O.⁸ The list is prescribed persons or classes of persons and prescribed circumstances for prescribed purposes. Now, I realize that there may be some non-lawyers in the audience, and I beg your indulgence and hope you will permit me to translate this legalese into non-legalese for you. I would interpret that particular clause, Paragraph O, to mean anybody. CCRA is going to give you the stuff.

A couple of days ago, April 9th, the Privacy Commissioner went to war about this.⁹ The Minister of CCRA announced on April 9th some changes. They are still going to keep it for six years. It will only be accessible for 72-hours. After that it will be accessible, but anonymized, which is a crock. What they do is take the names off, map the names to a number, and put it in a separate database. It is accessible with an extra step to go through. After that it is only used for security purposes. So, while it is anonymous, it can be re-personalized.

The Public Safety Act is not law. It is essentially a CCR database that gives the same sort of collection ability to Transport Canada.¹⁰ It allows Transport Canada to collect and then permits the Royal Canadian Mounted Police (RCMP) to access the information and to keep it a bit longer if it is related to transportation, security, or terrorist threats. By the way, air carriers have to disclose information. Immigration information can be shared for national security reasons. The Private Sector Privacy Act is amended to allow companies to disclose the information.¹¹ Otherwise, they are not allowed to without consent for national defense International affairs and all that sort of good stuff.

You start to see the idea that law enforcement is concerned about their ability to access electronic communications, and that is what the lawful access is trying to get at. The national I.D. card proposal, which includes biometric information as a means of communication when traveling abroad

⁸ Arrangement on the Recognition of Common Criteria Certificates (CCRA).

⁹ *Breakthrough for Privacy Rights*, PRIVACY COMMISSIONER OF CANADA, April 9, 2003, available at www.privcom.gc.ca/media/nr-c/2003/02_05_b_030408_e.asp

¹⁰ *Public Safety Act 2002*, Fact Sheet, FORMER PRIME MINISTER'S NEWSROOM ARCHIVE, April 30, 2002, available at www.pcobcp.gc.ca/default.asp?Language=E&Page=pmarchive&Sub=factsheets&Doc=psa.20020430_e.htm

¹¹ Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5; *Privacy Protection in the Private Sector*, Consultation Paper, BRITISH COLUMBIA MINISTRY OF MANAGEMENT SERVICES (2002), available at www.msar.gov.bc.ca/foi_pop/Privacy/psp_consult.pdf

was spurred by the U.S. Patriot Act requiring foreign citizens and Atlantic immigrants to have I.D. with integrated identification technologies such as biometrics. I understand Congress has rejected the idea of having national I.D. cards in the United States. Regardless, you are requiring us to seriously consider the idea. As I understand it, we are trying to get an exemption, whether that happens or not, I kind of hope so. I kind of like my passport.

BALANCING SECURITY AND PRIVACY

The facts are that there are bad people out there and they do bad things. We have to recognize that and deal with that. I respectfully submit that you cannot throw the baby out with the bath water. You have to balance some freedoms and especially privacy. It is justifiable to a point. The information has to be collected for specific purposes. The big fear and big danger is that the information will be used for other purposes. Hence, Paragraph O, if you look at the list in the Custom's Act, you can see they can disclose information like the passenger name information to environmental officials in a province for the enforcement of environmental legislation. What the heck does my traveling from London to Ottawa have to do with the environment? Somehow, if the environmental official wants to be able to see that according to the text of the Custom's Act she can. The idea here is that you have to be careful about the scale and breath of the collection. Scale being how many people. Breath being what information fields your collecting and how long you are going to hold the information. If it is accessible for a long period of time it becomes a database about that individual. If you can use that kind of framework to limit the collection of information, and the non-aggregation of personal information that is held by everyone, you will go some way about balancing the concerns that people have about the personal information that is being collected about them.

In conclusion the surveillance infrastructure is growing and the anti-terrorism measures basically have been used as an excuse. I do not know about the United States. I suspect David may say something along the same lines. Certainly, in Canada, it has been. Time frame is important. The Canadian time frame is certainly a lot shorter than the American time frame.

In large part, when we see CNN, Fox, and MSNBC and we see the graphics splashed behind the commentators; the war on terrorism. For a lot of Canadians that was just a graphic. What a lot of Canadians do not realize is that you folks do not see it that way. You Americans really are at war and a lot of Canadians do not see that. We are fighting terrorism, but it is not translated to that all out total effort of war. In the United States, it appears certainly to an outside observer like myself that is the case. When you talk about the kind of surveillance that people will accept in war time, it will not be accepted in peace time.

Pre 9-11, the privacy focus was on the private sector and it was EU driven. Post 9-11, it was focused on the public sector and it is U.S. driven. If you take the thesis that I presented to you and accept it, even then the perspective is important. At the end of day, do you trust the system? There will be people who do trust the system. The controls are in place. The security apparatus that says we only use the information for the purposes that we collected, which is national security, we only use it for that purposes. If you believe them, then you are going to be okay. If you do not believe them, you are not going to be okay. You are going to worry about it. You are going to see cynicism and an erosion of the values that one holds in the democratic society. I may not get this right, but I am reminded of a quote that came out of the Vietnam War, “We had to destroy the village in order to save it.” That is something to keep in mind when you talk about the Patriot Act and when we talk about anti-terrorism legislation. That what you intend to do may not result in what you want to do. On that note, I thank you very much for being an attentive audience.

