Security Versus Civil Liberties: The Preservation of Online Free Speech and Privacy in an Age of Global Terrorism

Extended Abstract

Richard S. Rosenberg

Department of Computer Science, University of British Columbia, Vancouver, BC Canada, V6T 1Z4. rosen@cs.ubc.ca

1. Introduction

It is now well into the second year of the war against terrorism in response to the terrible events of September 11, 2001 in the U.S. Not surprisingly the measures taken, primarily in the U.S., have once again raised the dilemma in democratic states of the degree to which security measures can compromise the civil liberties, which distinguish these countries from totalitarian ones. Simply put, for how long and for how forcefully can security measures be applied without risking those very values which are being defended? A number of legislative measures have been taken in Canada and the U.S. and these will be described. Even more importantly, the direct impact of these new laws will be traced and examples provided.

It is important and necessary to catalogue the immediate results of restrictive legislation on basic liberties of democratic societies, especially free speech and privacy. Such civil liberties can easily be exercised in times of both relative internal and external calm but the true mettle of a free society can only be measured when threats to civil order exert a "clear and present danger." One interesting analysis to be presented is the response to a discussion paper released by the Canadian Government at the end of August, 2002, titled "Lawful Access." The issues turn on requirements to be placed on Internet Service Providers (ISPs) to permit law enforcement officials to access Internet traffic of suspect ed individuals. The government has an interest in requiring ISPs to trap and hold information of one or more clients prior to providing sufficient evidence to obtain court orders, so-called data preservation. It may also have an interest in data retention, the trapping and storing of all Internet traffic of all clients for an extended period of time. Such actions would have a serious impact on online privacy and would also inhibit the exercise of free speech..

It is important to understand how basic rights are actually affected by laws intended to facilitate the actions of law enforcement officials in detecting and preventing subversive acts. Given that the Internet is the target of many of these laws, how they operate, how effective they are, and what their short and long term impacts are, must be determined for the good of society now and into the foreseeable future.

2. Legislation in Canada and the U.S.

Last year, I wrote about the first stages of the process of introducing legislation to combat terrorism in both Canada and the U.S.[1] A preliminary description of challenges

[1] Richard S. Rosenberg, "Is the Enemy Us? New threats to Privacy, Freedom of Information and Civil Liberties in the Age of Terrorism." In Klaus Brunnstein and Jacques Berleur (eds.), **Human Choice and Computers: Issues of Choice and Quality of Life in the Information Society**. IFIP

to civil liberties was presented and the task in this paper is to extend that analysis in order to identify, if possible, long term trends indicating that even in democratic societies, substantial compromises in the exercise of long-established rights have taken place. Obviously, space limitations preclude a thorough analysis but it is hoped that enough examples will be presented to make the point that new powers granted to the state, and its law enforcement agencies, have changed the ground rules and for the foreseeable future, rights for Canadians and Americans will be diminished. For purposes of this paper, basic rights are those enshrined in the Canadian Charter of Rights and the U.S. Bill of Rights, respectively. While global declarations of human rights are important and relevant, for most North Americans, they are also somewhat remote and non-applicable.

The USA PATRIOT Act of 2001[2] (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) was introduced and passed within three weeks of the September 11 tragedy. Given that the Act is about 300 pages in length, it must be the case that much of it was already drafted. Furthermore, the pressure to have it enacted quickly meant that the implications of its many sections could not possibly be understood by the legislators. Indeed, only over the past, almost two years have some of its threatening features become clear. A recent piece in the *Los Angeles Times*[3] describing an unexpected dinner adventure, at an Indian restaurant off Times Square in New York, is revealing.

> Suddenly there was a terrible commotion and five police officers in bulletproof vests stormed down the stairs. They had their guns drawn and were pointing them indiscriminately at the restaurant staff and at us. "Go to the back of the restaurant," they yelled. . . . Having some limited knowledge of the rights afforded to U.S. citizens, I asked why we were being held. The INS agent said we would be released once they confirmed that there were no outstanding warrants against us and our immigration status was OK. In pre-9/11 America, the legality of this would have been questionable. After all, the 4th Amendment states: "The right of the people to be secure against unreasonable searches and seizures." "You have no right to hold us," said Asher. But they explained that they did: This was a homeland security investigation under the authority of the Patriot Act. . . . When I asked to speak to a lawyer, the INS official told me I did have the right to a lawyer but I would have to be taken to the station for security clearance before being granted one. When I asked how long that would take, he replied with a coy smile: "Maybe a day, maybe a week, maybe a month."

In Canada, the following pieces of legislation have either been passed or are being debated and represent Canada's response to the events of September 11, 2001: [4]

- Bill C-36, the *Anti-terrorism Act*, received Royal Assent on 18 December 2001.
- On 28 November 2001, the House of Commons unanimously consented to a motion to delete from Bill C-42 section 4.83 in clause 5 amending the *Aeronautics Act*. The same day, that section was introduced as Bill C-44 in order to provide for speedier passage

---

17th World Computer Congress – TC9 Stream/International Conference, August 25-30, 2002, Montreal, Quebec, Canada. Boston, MA: Kluwer Academic Publishers, pp. 183-194, 2002.

2 USA Patriot Act (2001). Available at http://www.epic.org/privacy/terrorism/hr3162.html

3 Jason Halperin, "Feeling the Boot Heel of the Patriot Act," *The Los Angeles Times*," May 2, 2003. Available at http://www.latimes.com/news/opinion/la-oe-halperin2may02,1,4171430.story?col1=la%2Dheadlines%2Doped%2Dmanual

4 "Bill C-17: The Public Safety Act, 2002," Legislative Summary, Parliamentary Research Branch, November 15, 2002. Available at http://www.parl.gc.ca/37/2/parlbus/chambus/house/bills/summaries/C17-e.pdf

than consideration as part of Bill C-42 would have allowed for. It received Royal Assent on 18 December 2001.

- Bill C-17, the proposed *Public Safety Act, 2002* received first reading in the House of Commons on 31 October 2002. It replaces Bill C-55, which died on the *Order Paper* when the first session of the 37th Parliament ended on 16 September 2002. Bill C-55, in turn, replaced Bill C-42, which was given first reading on 22 November 2001; it received significant criticism and the Government did not proceed with it.

In Rosenberg (2002),[5] the tortured passage of the *Anti-terrorism Act* is discussed. It should be noted that in its first reading, none of the restrictions on civil liberties were to be reviewed in the near future; that is, it lacked a sunset clause. Computer and Internet related sections of this Act, are given as follows: [6]

> The amended version of Bill C-36 contains several sections related to computers, computer networks, and Internet related issues. For a measure of completeness, it is well worth describing at least two of these. Section 320 of the *Criminal Code* is amended by the addition of the following section:
>
> **320.1** (1) If a judge is satisfied by information on oath that there are reasonable grounds for believing that there is material, that is, hate propaganda within the meaning of subsection 320(8) or data within the meaning of subsection 342.1(2) that makes hate propaganda available, that is stored on and made available to the public through a computer system within the meaning of subsection 342.1(2) that is within the jurisdiction of the court, the judge may order the custodian of the computer system to
>
> (a) give an electronic copy of the material to the court;
>
> (b) ensure that the material is no longer stored on and made available through the computer system; and
>
> (c) provide the information necessary to identify and locate the person who posted the material.
>
> A judge is now able to make a unilateral decision on what qualifies as hate speech under the Criminal Code for material on the Internet.
>
> The *Canadian Human Rights Act* is amended by the replacement of Subsection 13(2) by the following
>
> (2) Subsection (1) does not apply in respect of any matter that is communicated in whole or in part by means of the facilities of a broadcasting undertaking but does apply to a matter that is communicated by a computer or a group of interconnected or related computers, including the Internet, or any similar means of communication.
>
> Now, Subsection (1) refers to hate messages, that is, "any matter that is likely to expose a person or persons to hatred or contempt by reason of the fact that that person or those persons are identifiable on the basis of a prohibited ground of discrimination." Thus as a result of this amendment, the communication of hate messages by means of broadcasting systems is still not a "discriminatory practice" but doing so over the Internet is. How will Canadians be safer as a result of this amendment and why does the Internet merit such special treatment whereas traditional broadcasting media do not?

3. Privacy and Free Speech Issues

In what follows we will identify a variety of U.S. threats to civil liberties followed by one example from Canada. American are regularly surveyed about their views on measures taken to protect them from terrorist activities; the following are highlights of a survey carried out about one year after September 11 and of particular interest given its focus on the Internet. A few highlights are given as follows: [7]

---

[5] **Op. cit.** "Is the Enemy Us?

[6] **Ibid.**

[7] "One Year Later: September 11 and the Internet," Pew Internet & American Life Project, September 5, 2002. Available at http://www.pewinternet.org/reports/pdfs/PIP_9_11_Report.pdf

- More than two-thirds of Americans believe that the government should be granted wide privileges in deciding what information to post on government agency Web sites and what information to keep off government sites for fear it will help terrorists.
- Some 47% say that the act of withholding or removing information from government Web sites will not make a difference in deterring terrorists;
- 47% of Americans believe the government should not have the right to monitor people's Internet use and 45% say the government should have that right. A majority of Internet users oppose government monitoring of people's email and Web activities.

It seems clear that in spite of the deep concern about terrorism, most Americans value their rights and are reluctant to compromise them. However, over the past two years the U.S. government has taken a number of steps, which have been challenged by most civil liberties organizations as serious violations of basic constitutional rights. Among these are the following:

- Early last week, the program's Web site indicated that Operation TIPS, which stands for Terrorism Information and Prevention System, would begin in selected American cities next month. . . ELI RIOS JR. is just the kind of guy Uncle Sam wanted on the front lines of Operation TIPS, the Justice Department's ill-fated plan to encourage meter readers, truck drivers, cable guys and other workers whose jobs routinely take them through the nation's neighborhoods to report signs of terrorism to a national hotline. . . The Bush administration presented Operation TIPS as sort of a national version of a neighborhood block-watch, a universally praised program that helps communities foil common criminals.[8]
- Said Homeland Security chief Tom Ridge: "The last thing we want is Americans spying on Americans. That's just not what the president is all about, and not what the TIPS program is all about." [9]
- Barbara Olshansky was at a Newark International Airport departure gate last May when an airline agent at the counter checking her boarding pass called airport security. Olshansky was subjected to a close search and then, though she was in view of other travelers, was ordered to pull her pants down. . . . But now, for the first time, a spokesman for the new Transportation Security Administration [TSA] has acknowledged that the government has a list of about 1,000 people who are deemed "threats to aviation" and not allowed on airplanes under any circumstances. And in an interview with Salon, the official suggested that Olshansky and other political activists may be on a separate list that subjects them to strict scrutiny but allows them to fly. . . "We have a list of about 1,000 people," said David Steigman, the TSA spokesman. The agency was created a year ago by Congress to handle transportation safety during the war on terror. "This list is composed of names that are provided to us by various government organizations like the FBI, CIA and INS. . . We don't ask how they decide who to list. Each agency decides on its own who is a 'threat to aviation'." [10]
- The Patriot Act's Section 215 requires American bookstores and public libraries to surrender to the FBI lists of books or other materials that customers or patrons have accessed. As with past FBI library watch campaigns, libraries are instructed under order of law to not disclose the FBI's presence or interest in the reading habits of particular patrons. Alerting patrons, or the public of the occurrence of an FBI library visit brings threats of arrest. Some library's have adopted a policy of hanging signs in library entry ways declaring "The FBI has not visited here today," with community understandings that these signs will be removed upon an FBI visit. . . The American Library Association's Code of Ethics explicitly calls for the protection of intellectual freedom and instructs librarians to "resist all efforts to censor library resources," and to "protect each library user's right to privacy and confidentiality with respect to information

[8] Andy Newman, "Citizen Snoops Wanted," *The New York Times*, July 21, 2002.
[9] "Postal Service Opposes Citizen Spy Program," Associated Press, July 17, 2002. Available at http://www.foxnews.com/story/0,2933,5784,00.html
[10] Dave Lindorff, "Grounded," Salon, November 15, 2002. Available at http://archive.salon.com/news/feature/2002/11/15/no_fly/index_np.html

sought or received and resources consulted, borrowed, acquired or transmitted". Over a year ago governmental repository libraries quietly began complying with censorial governmental demands to remove specific materials that were thought to be of possible use to terrorists. Today we find the FBI resurrecting its old discredited Library Watch Program in the name of fighting terrorism with only words of complain, not acts of defiance from American librarians. [11]

- School administrators have told the group, called the Che Cafe Collective, that linking to a site supporting the Revolutionary Armed Forces of Columbia (FARC) would not be permitted because it violated federal law. In a letter to the Che Cafe Collective, UCSD University Centers Director Gary Ratcliff said the hyperlink violated a law that bans "providing material support to support terrorists." Ratcliff warned that the student organization would face disciplinary action if it did not immediately remove the link to FARC. "The concern of the institution is that this could be interpreted as a violation of the law," Ratcliff said in an interview Wednesday. "What we're trying to be is pro-active here. If the FBI decided to pay attention to this matter, the repercussions would go way beyond their group because we're providing network services." The law in question is one section of the USA Patriot Act, signed by President George W. Bush last October, which outlaws providing "material support or resources" to foreign terrorists who have been placed on a State Department list. Material support is defined as money, lodging, training or "communications equipment." [12]
- If you think the Bill of Rights is just so much scrap paper, and the separation of powers doctrine has outlived its usefulness, then the USA PATRIOT Act, passed overwhelmingly on Oct. 25, is the right recipe to deal with terrorists. On the other hand, if you are concerned about Fifth Amendment protection of due process, and Fourth Amendment safeguards against unreasonable searches and seizures, then you should be deeply troubled by the looming sacrifice of civil liberties at the altar of national security. . . Yet the more acute objections to the new statute are substantive, not procedural. They fall into three main categories. First, any law with the potential to dramatically alter conventional notions of individual freedom should fastidiously guard against abuse. Second, if the new rules are at all justifiable, they are defended as a necessary instrument of anti-terrorism. If so, why do many of the provisions apply not only to suspected terrorist acts but also to everyday national security investigations and even ordinary criminal matters? . . Third, laws that compromise civil liberties must be revisited periodically to assure that temporary measures, undertaken in response to a national security emergency, do not endure longer than necessary. Such laws must contain sunset clauses; that is, the law should expire automatically within a short time of enactment - thus imposing on government the continuing obligation to justify its intrusions. [13]

There is much more but the point is clear; even commentators on the political right in the U.S., for example Robert Levy of the Cato Institute and the author of the last item, are appalled by the wide net cast by the USA PATRIOT Act. Concerns, on both the left and certain parts of the right, overlap in terms of a fear that well-established rights may be lost forever. One last important example must be mentioned, namely the Total Information Awareness (TIA) System, managed by the Department of Defense's Defense Advanced Research Projects Agency (DARPA). Ironically, this Agency was largely responsible for the creation and growth of the Internet, in its early days. TIA is a

---

[11] David H. Price, "Prostrate to the Patriot Act, Librarians as FBI Extension Agents," CounterPunch, March 5, 2003. Available at http://www.counterpunch.org/price03062003.html

[12] Declan McCullagh, "University Bans Controversial Links," Cnet News.com, September 25, 2002. Available at http://news.com.com/2100-1023-959544.html

[13] Robert A. Levy, "The USA PATRIOT Act: We Deserve Batter," Cato Institute, November 11, 2001. Available at http://www.cato.org/current/terrorism/pubs/levy-martial-law.html

massively ambitious program and as such, it will have a serious impact on privacy and free speech rights. The program is described by DARPA as follows: [14]

> The Total Information Awareness (TIA) program is a FY03 new-start program. The goal of the Total Information Awareness (TIA) program is to revolutionize the ability of the United States to detect, classify and identify foreign terrorists – and decipher their plans – and thereby enable the U.S. to take timely action to successfully preempt and defeat terrorist acts. To that end, the TIA program objective is to create a counter-terrorism information system that: (1) increases information coverage by an order of magnitude, and affords easy future scaling; (2) provides focused warnings within an hour after a triggering event occurs or an evidence threshold is passed; (3) can automatically queue analysts based on partial pattern matches and has patterns that cover 90% of all previously known foreign terrorist attacks; and, (4) supports collaboration, analytical reasoning and information sharing so that analysts can hypothesize, test and propose theories and mitigating strategies about possible futures, so decision-makers can effectively evaluate the impact of current or future policies and prospective courses of action.

William Safire, the conservative columnist for *The New York Times*, wrote a highly critical piece on November 14, 2002, followed some three months later by another article, updating Congressional steps taken to identify the scope and purposes of the TIA program. Consider his remarks, as follows: [15]

> Readers with keen memories will recall a blast in this space three months ago at the proposed "Total Information Awareness" project, which the Pentagon proudly described as "a virtual, centralized grand database.'" In the name of combating terrorism, it would scoop up your lifetime paper trail -- bank records, medical files, credit card purchases, academic records, etc. -- and marry them to every nosy neighbor's gossip to the F.B.I. about you. The combination of intrusive commercial "data mining" and new law enforcement tapping into the private lives of innocent Americans was described here as "a supersnoop's dream.". . . An amendment to the budget bill by Senator Ron Wyden, Democrat of Oregon, co-sponsored by Chuck Grassley, Republican of Iowa, put a bit in the mouth of the Pentagon's runaway horse. The Wyden amendment held up funding for the Total Information Awareness penetration of the American home until the administration (1) explained it in detail to Congress, including its impact on civil liberties, and (2) barred any deployment of the technology against U.S. citizens without prior Congressional approval. One hundred senators voted in favor.

In Canada, the debate is much more muted. While civil liberties organizations have concerns, and rightly so, for the most part, the Canadian population is generally silent. However, one issue did seem to evoke some concern, at least from Canada's Privacy Commissioner George Radwanski and the Privacy Commissioners of Ontario and British Columbia. Bill C-17 authorized the creation of an air travellers' CCRA database (Canada Customs and Revenue Agency) to store API/PNR information (Advance Passenger Information/Passenger Name Record). The criticism focused on the nature of the information to be stored, the length of time it would be kept, and who would have access to it. It seemed that although the collection was motivated by security concerns, its primary use would be for traditional criminal investigations. The Minister of National Revenue Elinor Kaplan rejected criticisms but in April 2003, she announced

---

[14] "Total Information Awareness (TIA) System," Defense Advanced Research Projects Agency,(Date Unknown). Available at http://www.darpa.mil/iao/TIASystems.htm

[15] William Safire, "Privacy Invasion Curtailed," *The New York Times*, February 13, 2003, Section A, page 41.

new procedures, which were welcomed by the Canadian Privacy Commissioner, but not by some others, as a satisfactory resolution of his criticisms. [16]

4. On the Horizon

During the past year new threats and assaults on privacy and free speech have occurred or are being planned. Among these, in the U.S., is the so-called Patriot Act II, a follow up to the original Act. In Canada, the idea of a National Identity Card has been floated and a discussion paper and hearings have been held on "Lawful Access" to information held by Internet Service Providers.

The Patriot Act II. document was publicized by the non-partisan Center for Public Integrity, earlier this year, with the claim that it was a draft of forthcoming government policy called the Domestic Security Enhancement Act of 2003; the government claimed that it was a work-in-progress.[17] Some of the powers in this proposal give the government the right to [18]

- Conduct domestic wiretapping without court order for 15 days following a congressional authorization of use of force or an attack on the United States.
- Access a citizen's credit reports without a subpoena.
- Abolish federal court "consent decrees" that limit police surveillance of non-criminal organizations and public events.
- Criminalize the use of encryption software in the commission or planning of a felony.
- Collect DNA from suspected terrorists and indeed from any individual whose DNA might assist terror investigations.
- Extend authorization periods for secret wiretaps and Internet surveillance.
- Ease restrictions on the use of secret evidence.

The Lawful Access – Consultation Document was released by Justice Canada on August 25, 2002 with a call for comments. [19] A definition follows, taken from the Consultation Document:

> Lawful Access is an important and well-established technique used by law enforcement and national security agencies to conduct investigations. In the context of telecommunications in Canada, it consists of the interception of communications and search and seizure of information carried out pursuant to legal authority . . . Lawfully authorized interception and the search and seizure of documentation, computer data, and other information is used frequently by law enforcement agencies to investigate serious crimes such as drug trafficking, child pornography, murder, money laundering, price fixing and deceptive telemarketing.

Furthermore, the document proposes that,

- ISPs have the technical ability to monitor all Internet communications.

---

[16] "Breakthrough for Privacy Rights," News Release, Privacy Commissioner of Canada, April 9, 2003. Available at http://www.privcom.gc.ca/media/nr-c/2003/02_05_b_030408_e.asp

[17] Charles Lewis and Adam Mayle, "Justice Dept. Drafts Sweeping Expansion of Anti-Terrorism Act," The Center for Public Integrity, February 7, 2003. Available at http://www.publicintegrity.org/dtaweb/report.asp?ReportID=502&L1=10&L2=10&L3=0&L4=0&L5=0

[18] "A Chilly Response to 'Patriot II'," Wired News, February 12, 2003. Available at http://www.wired.com/news/politics/0,1283,57636,00.html

[19] "Lawful Access – Consultation Document," Department of Justice, Government of Canada, August 25, 2002. Available at http://www.canada.justice.gc.ca/en/cons/la_l/law_access.pdf

- ISPs be prepared to store specific Internet traffic for up to six months without a warrant. [Data preservation]
- E-mail be defined appropriately for interception purposes.
- Privacy of Canadians be preserved.

The major concerns for civil liberties advocates include the following:

- Although only data preservation is being proposed, there is some evidence that data retention is close behind. [Data retention is the saving of **all** Internet traffic carried by a given ISP.]
- In the context of past and current assaults on privacy, Lawful Access takes on a more dangerous tone.
- The definition of service provider is not sufficiently precise: Are universities, colleges, and public libraries service providers? If so, their patrons – students and the general public – are subject to proposed provisions.
- What about anonymous use, now available?
- Will encryption policies now be revisited?

A submission was made to the Department of Justice by Electronic Frontier Canada with the help of the U.S. Electronic Freedom Foundation. [20]

Finally, we turn briefly to a proposal floated by the Minister of Citizenship and Immigration that Canadians would be better off with all its citizens required to carry a National Identity card. For example, it was stated that identity theft would be reduced, terrorists would be more readily apprehended, and Canadians would find it easier to enter the U.S. No justification was given for these claims and it is typical of most efforts in this area that measures ostensibly directed towards dealing with terrorists find their primary use in dealing with traditional criminal acts.

Such National ID cards are used currently in many countries and have also been proposed for many others. Shortly after September 11, an effort was undertaken in the U.S. to adopt an ID card but it failed as have all previous efforts. As part of hearings across the country to review proposals for changes in the Citizen and Immigration Act, members of Parliament also received comments about a Canadian National ID card. As part of this process, and as a vice-president of Electronic Frontier Canada, I made a presentation at hearings held in Vancouver. [21] Not surprisingly, my argument was in complete opposition to the proposal.

5. Conclusions

It is inevitable that in the aftermath of crises such as September 11, concern for the security of the nation will (seem to) overweigh individual privacy rights. The Canadian Government has introduced a number of bills that raise serious privacy issues and in the context of such legislation as well as concerns about the Canadian Customs and Revenue Agency (CCRA) database on foreign travel activities and the Lawful Access discussion paper, the ID card proposal strikes many that the government is clearly over-reacting. Simply put, Canadians neither need nor desire a National Identity Card. It is being advertised as a solution to identity theft and as a means to improve the chances of identifying and apprehending terrorists.

---

[20] Available at http://www.efc.ca/pages/surveillance/lawfuldoc.

[21] Richard S. Rosenberg, "Appearance Before the Standing Committee on Citizenship and Immigration, Re: National Identity Card," February 19, 2003. Available at http://www.efc.ca/pages/privacy/ParlPresFeb19.pdf

In spite of its claims as the world's premier democracy, the U.S. has no qualms about criticizing one of its closest international friends for being too concerned about the privacy rights of its citizens. A commentary on a recent U.S. State Department report on global terrorism, notes the following: [22]

> The United States says the lack of funding for police and restrictive privacy legislation in Canada are frustrating probes of political extremists. . . The State Department report on global terrorism for 2002 suggests that while Canada has been helpful in the fight against terrorism, it doesn't spend enough on policing and places too much emphasis on civil liberties. It says "some U.S. law enforcement officers have expressed concern" about Canadian privacy laws. The U.S. officers feel those laws, as well as funding levels for law enforcement, "inhibit a fuller and more timely exchange of information and response to requests for assistance," the report says. "Also, Canadian laws and regulations intended to protect Canadian citizens and landed immigrants from government intrusion sometimes limit the depth of investigations."

That the U.S. should criticize Canada for placing "too much emphasis on civil liberties," is the height, or depth perhaps, of irony. It raises the obvious question of whether the concern with security has so overwhelmed long valued adherence to basic rights that the U.S. has, one hopes temporarily, lost sight of what it is defending.

[22] Jim Bronskill, "U.S. Says Canada Cares too much about Liberties," Ottawa Citizen, May 1, 2003. Available at http://www.canada.com/national/story.asp?id=78A2260B-4770-4682-BE60-E6FE1D3B8144