J O E B A P T I S T A
4 0 4 - 3 0 3 A Y L M E R S T R E E T
P E T E R B O R O U G H , O N T A R I O C A N A D A K 9 J 7 K 5

September 9, 2002

Mr. George Radwanski
Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario K1A 1H3

and

Mr. John Reid
Information Commissioner of Canada
Place de Ville, Tower B
112 Kent Street, 22nd Floor
Ottawa, Ontario K1A 1H3

Dear Messrs. Radwanski and Reid:

RE: **Electronic privacy issues affecting Canadians, business and government.**

I am writing you concerning a potential invasion of privacy to Canadian and global users of internet services that support the United States namespace infrastructure to resolve domain names to internet protocol addresses. This vulnerability exists due to the failure of the United States government in properly addressing security and privacy issues involved in root operations. At the present time over 70% of global internet traffic is directed by appointed agents of the United States Department of Commerce. At this time, Canada supports the efforts of the U.S. Department of Commerce through the participation of Ms Lisa Jacobson a Policy Analyst in the Business and Regulatory Analysis Telecommunications Policy unit of Industry Canada.

Ms. Jacobson represents Canada's interests at the Government Advisory Committee to the Internet Corporation for Assigned Name and Numbers (ICANN).ICANN is an agent and contractor of root services to Commerce.

I expressed my concerns in a letter to Mr. Donald Evans the Commerce Secretary this past January 21, 2002 with respect to the operation of the root servers by Commerce:

> ***"We have also identified potential risks to anyone who uses the legacy roots. The continued operation of these roots by Commerce can be subject to abuse. It is technically possible to use root servers to redirect traffic to a single point where it can be monitored. This gives your department the unprecedented power to violate the privacy of any individual, group, or government using the U.S. root system to navigate the Internet. Recent changes to U.S. law encourage the interception of Internet traffic. This in our opinion poses a serious threat to the integrity, security and privacy of Internet users."***

To date we have not received a reply back from Secretary Evans. I also email our airheads in parliament on this but failed to generate any interest except for the usual marketing request asking if I was in their riding. When a nations' security and the privacy of its citizens are at stake I doubt my address is of any issue. I hope that your positions as Privacy and Information Commissioners impresses

on you the danger our nations infrastructure is in from it's reliance on U.S. centric agencies to provide navigational infrastructure to government and business computer systems.

I am pleased to say that members of the European Union were not only understanding but did their best to understand the implications of our communication.

I hope the following backgrounder provides you with an understanding of the technical issues involved and the urgency that the situation be addressed and corrected promptly.

Backgrounder - Roots and the Domain Name System

Every computer connected to the Internet uses the domain name system (DNS) to navigate. When a computer attempts to contact a server on the Internet, it uses a domain name to look up the numeric Internet protocol address of the server it wants to reach. This process is done through the DNS by a series of trusted servers and the master server that everyone trusts is called the root server.

The following diagram provides an example of the process involved when a users browser uses the DNS to connect to a target server.

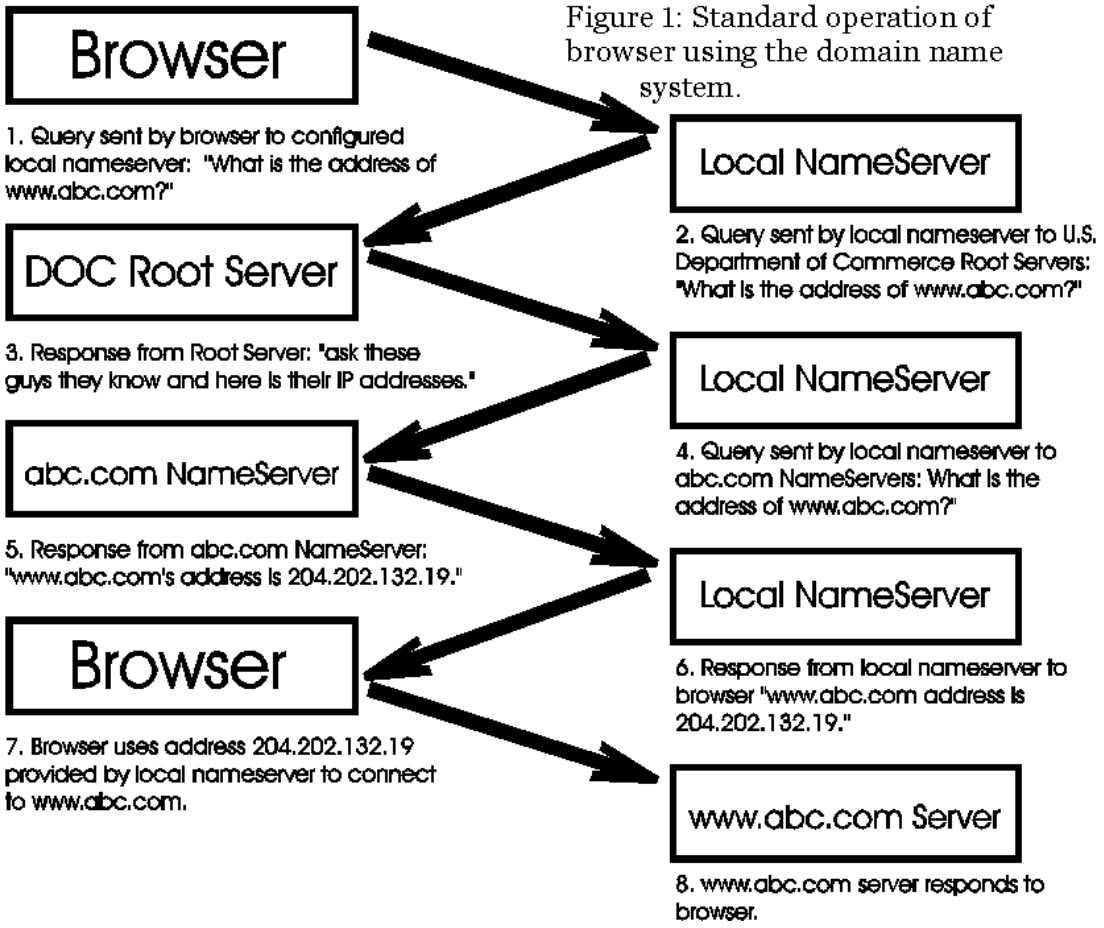

Figure 1: Standard operation of browser using the domain name system.

The users browser assumes the information it receives from it's DNS query is correct and that the servers providing the information can be trusted to provide correct answers. Under normal circumstances the users browser connects to the correct server on the Internet.

However, it is possible for a root server operator to modify the response to the browsers query and in turn use a proxy server to intercept traffic. Figure 2 provides a procedure that can redirect specific or general Internet traffic using a trusted root server system

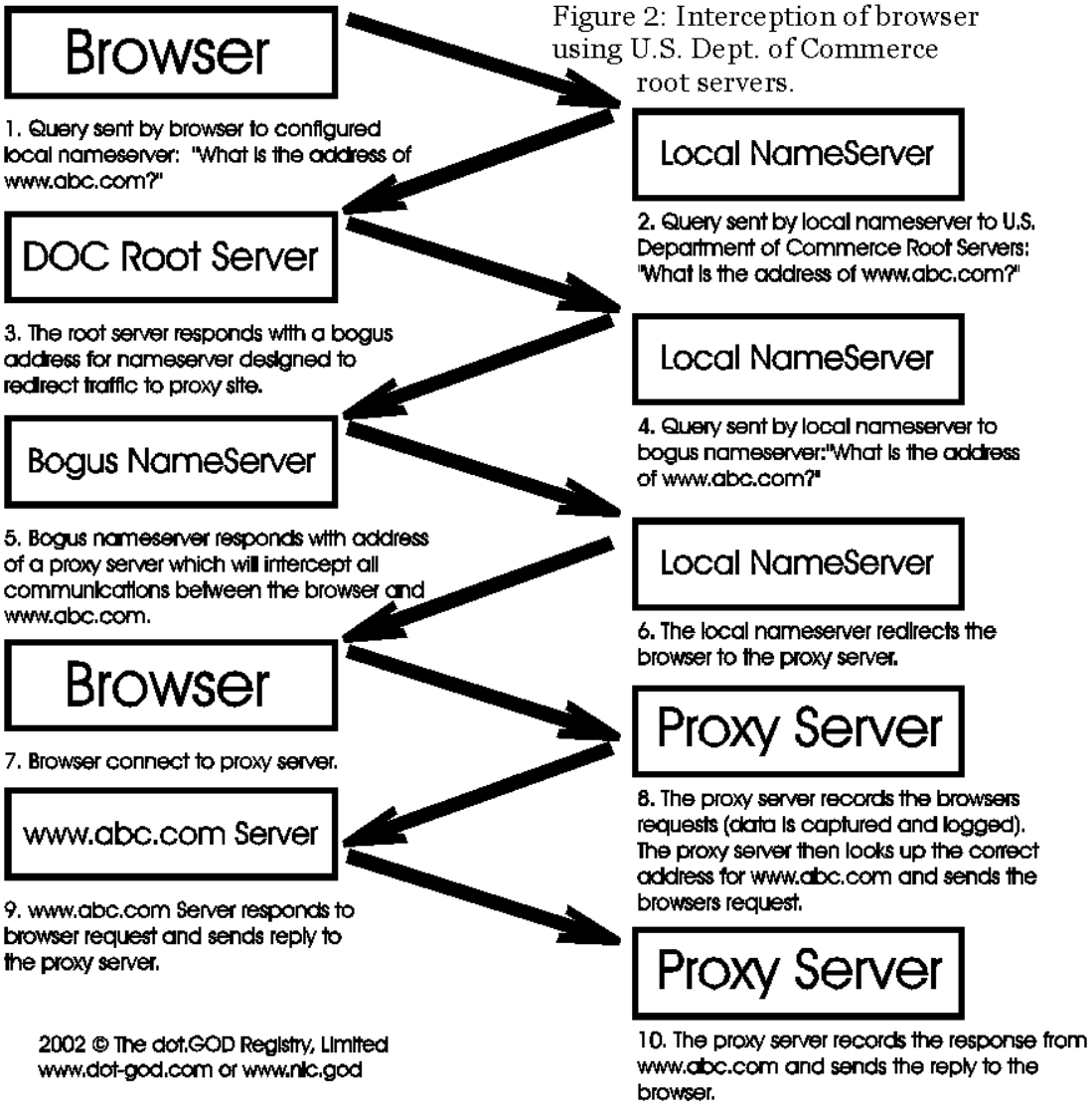

Figure 2: Interception of browser using U.S. Dept. of Commerce root servers.

Technology now exists which can target one specific user or entire networks of computers. The trick is to know the local nameservers of the targeted systems. We sites can also be monitored for traffic and their data archived for later investigation.

It is also possible for Internet Service Providers to use their local nameservers to intercept traffic through a proxy located on the local network or export the traffic to a proxy server at a law enforcement agency. I can see this sort of surveillance method being deployed in future, to monitor user activity.

Using the DNS to intercept traffic is common in some countries. The most novel use seems to have originated in the orient where ISP's duplicate web sites containing the same content as the official web site. There is a profit motive behind this type of interception in which he ISP acts as the sales agent.

I have also heard of instances where an ISP redirects all user traffic through a proxy agent which replaces web advertising content with ISP based ad copy on the fly. Again and attempt at generating additional revenue where the motive is profit driven.

Figure three outlines the processes that can be used by ISP's to redirect user traffic through local nameservers and proxy agents.

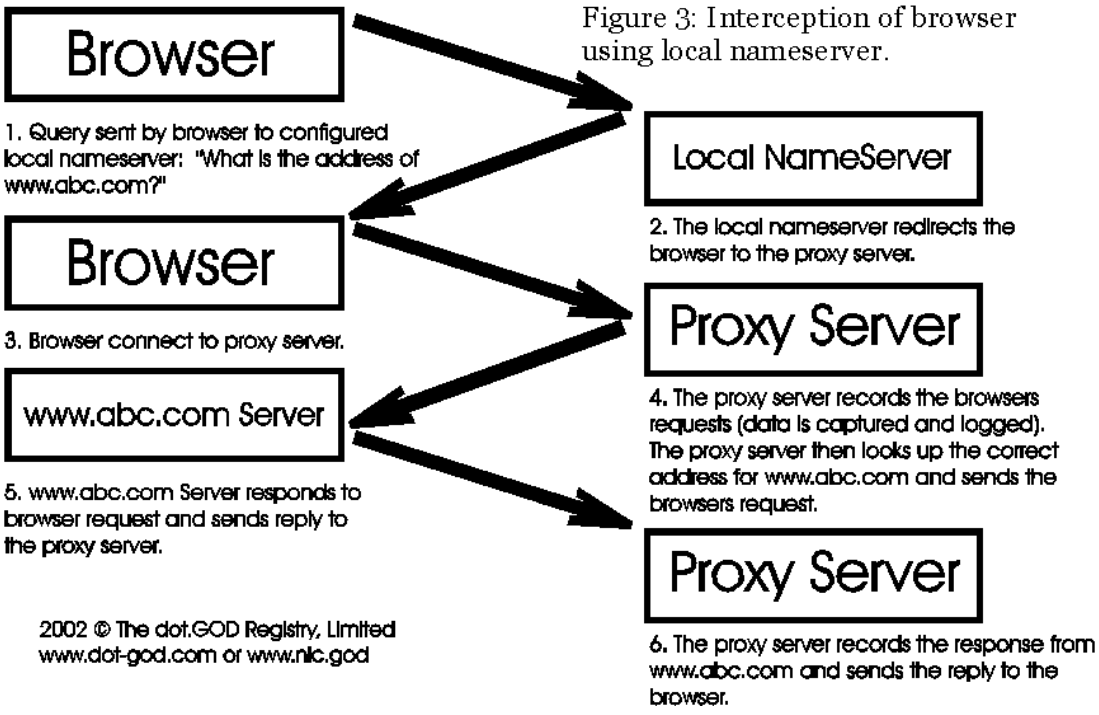

Figure 3: Interception of browser using local nameserver.

I hope commissioners that you understand the magnitude of the problem and the potential abuses if we do not address these technical issues.

A simple solution

On a positive note, it is a simple matter to correct this security vulnerability, and the governments' reliance on U.S. government provided directory services can be replaced with trusted local directory services. The government of Canada should simply run its own secure root server system. I would like you; Commissioner Reid and Radwanski, to assist us in bringing this issue to the attention of a responsible individual in our federal government who can investigate fix the problem.

Users can also protect themselves from having their sessions high jacked by reconfiguring their computer systems to a trusted root service or domain nameserver provider of their choice. The government of Canada may wish to consider making its root infrastructure available to the Canadian Public at large.

It would also be beneficial if the government were to provide the Canadian Internet community with assistance in securing their communications.

An example of a Root Interception

It is our intention to email you evidence attached to this correspondence of the type of abuse which can result when information is intentionally harvested by a root operator through interception. These logs and data records were collected from June 11 to 15, 2001.

The logs originated from a root interception I conducted on the users of Diebold, Inc., an American company listed on the New York Exchange. The interception was on behalf of Planet Communications & Computing Facility, an infrastructure provider who owned the physical Internet protocol addresses on which the Diebold root servers were platformed. These logs are significant and an excellent example of the type of abuse users can expect from an insecure root server system.

Root interception uses the same principles outlined in figure 2 above except all browsers and users are redirected to one specific host that cancels their Internet session. I anticipate you will find these logs useful in understanding the privacy issues I have flagged in this correspondence.

In closing I hope both of you can assist me in getting this issue properly addressed through the correct bureaucratic channels. I ask you to investigate and validate the technical claims I have listed here and have this problem fixed.

.

Sincerely,

Joe Baptista

CC: Lisa Jacobson jacobson.lisa@ic.gc.ca