March 12, 2004

CENTER FOR DEMOCRACY & TECHNOLOGY
Working for Civil Liberties on the Internet

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

Governor Olene Walker
210 State Capitol
Salt Lake City, Utah 84114

Dear Governor Walker:

The Utah Legislature recently passed HB 323, the "Spyware Control Act," in response to concerns about invasive and deceptive software applications sometimes known as "spyware." The Center for Democracy and Technology applauds the legislature's attention to this serious and rapidly growing threat to Internet users' privacy and their control over their computers and Internet connections. However, we believe the current bill is premature. We urge you to veto it, and to ask the legislature to conduct further study and then adopt a new bill with stronger and more focused protections for consumers, after the definitional difficulties surrounding spyware have been worked out.

CDT is a non-profit, public interest organization dedicated to preserving and promoting privacy and other democratic values and civil liberties on the Internet. We have been a leader in the policy debate about the issues raised by so-called "spyware." At the federal level, we have been engaged in the early legislative, regulatory, and self-regulatory efforts to deal with the spyware problem. We have been active in public education efforts to highlight the serious transparency and user control issues raised by these invasive applications.[1]

CDT strongly supports the premise of HB 323, that users should have meaningful notice and choice regarding the applications that run on their computers. However, CDT has several concerns about how this bill may impact consumers in practice:

---

[1] *See, e.g.*, "The Spies in Your Computer," *New York Times* Editorial, February 18, 2004 (arguing that "Congress will miss the point [(in spyware legislation)] if it regulates specific varieties of spyware, only to watch the programs mutate into forms that evade a narrowly tailored law. A better solution, as proposed recently by the Center for Democracy and Technology, is to develop privacy standards that protect computer users from all programs that covertly collect information that rightfully belongs to the user."); John Borland, "Spyware and its discontents," *CNET.com*, February 12, 2004 ("In the past few months, Ari Schwartz and the Washington, D.C.-based Center for Democracy and Technology have leapt into the front ranks of the Net's spyware-fighters."); CDT's "Campaign Against Spyware," http://www.cdt.org/action/spyware/action (calling on users to report their problems with spyware to CDT; since November 2003, CDT has received over 250 responses).

- Drafting appropriate notice and consent requirements for consumer software raises difficult definitional issues. The definition of "spyware" in HB 323 may be both over- and under- inclusive, negatively impacting many legitimate practices, while failing to cover many of the worst offenders. These definitional questions are the subject of ongoing discussions among industry groups, in federal regulatory bodies, and in Congress. The Federal Trade Commission is holding a workshop in April on "spyware" where it will be raising the question of "Defining and Understanding Spyware." CDT is currently leading discussions among consumer groups, ISPs, consumer software companies, anti-spyware technology vendors, and advertising companies regarding definitions relating to consumer software and spyware, in preparation for the FTC's workshop. We believe legislation is premature before these efforts have resolved the definitional issues.

- The specific requirements for presentation of notice in HB 323 are weak, and could set a bad precedent for what constitutes acceptable notice for consumers. Many "spyware" programs already provide nominal disclosure to consumers, hidden in long and legalistic licensing agreements. These types of notice would appear to fulfill the requirements of HB 323, although they fail to provide meaningful notice or choice to consumers.

- The bill offers few enforcement provisions that can actually protect consumers. The bill does not provide for a private right of action by consumers who are impacted by the installation of "spyware," nor does it allow the attorney general to take action against offending companies. Since many of the companies involved in the distribution of spyware are already committing fraud by deceiving consumers, HB323 may actually have the unintended effect of confusing cases where individuals or the attorney general can take action today.[2]

CDT is also concerned about problems that could be created by the patchwork of different notice and consent regimes that would result from addressing the "spyware" problem at the state level. The requirements set forth in HB 323, or in other similar bills, will have wide ranging effects on the design of consumer software including operating systems, web browsers, and other applications. We believe government may have an important role in defining the notice and consent standards to which programs should be held, and we understand the impetus for state legislation to clarify these standards in the

---

[2] *See, e.g*. CDT's *Complaint and Request for Investigation, Injunction, and Other Relief*, in the Matter of MailWiper, Inc., and Seismic Entertainment Productions, Inc., February 11, 2004 (available at http://www.cdt.org/privacy/20040210cdt.pdf).We have been told that some state attorneys general may be looking into this and similar cases.

absence of federal action. However we believe this issue represents a core interstate commerce issue and therefore a federal solution, if possible, is preferable.

CDT emphasizes that many of the invasive "spyware" applications that HB 323 would cover are already illegal under existing federal and state statutes. Enforcement of these statutes against "spyware" applications has so far been limited. CDT believes the best first step to fight these programs is better enforcement of existing laws, and states have an important and immediate role to play in this regard. Given the concerns with HB 323 that we have outlined, we believe that consumers will be best protected, not by premature adoption of new laws before the problem is adequately defined, but by increased efforts to bring cases under standing fraud statutes.

Sincerely,

Ari Schwartz
Associate Director