For release 9 a.m. ET (6 a.m. PT), Monday, 4/22/13

Contact: John M. Simpson, 310-392-7041

Consumer and Privacy Groups Endorse Rockefeller, Blumenthal Do-Not-Track bill

WASHINGTON, DC – A coalition of six consumer and privacy public interest groups today praised Sen. Jay Rockefeller (D-W VA) and Sen. Richard Blumenthal (D-CT) for introducing a Do-Not-Track bill, which would charge the Federal Trade Commission with establishing standards by which consumers could tell online companies, including mobile applications, that they do not want their information collected.

The Senate Commerce Committee will hold a hearing on the status of the development of voluntary Do-Not-Track standards at 2:30 p.m. Wednesday, April 24. Under the Rockefeller-Blumenthal bill, similar to legislation Rockefeller introduced in 2011, the FTC would be charged with ensuring that companies respect a consumer's Do-Not-Track choice.

The groups, which include The Center for Digital Democracy, Consumer Action, Consumer Federation of America, Consumer Watchdog, Privacy Rights Clearinghouse and U.S. PIRG, said in a statement:

> "It's now clear that legislation is necessary to ensure consumers get the protection they deserve and expect. Self-regulatory efforts to develop a Do-Not-Track standard have stalled. The Rockefeller-Blumenthal bill may spark action in such forums as the World Wide Web Consortium (W3C), but at the end of the day, we'll need legislation to get this done. Industry has had no real incentive to agree to a meaningful standard.
>
> "The attitude had been, let's give self-regulation a chance. We've spent 18 months and self-regulation is not working. Now is the time for legislative action and we welcome the senators' commitment to getting Do Not Track done."

A year ago the FTC issued its report "*Protecting Consumer Privacy in an Era of Rapid Change*," which called for the implementation of a Do-Not-Track mechanism. Instead of seeking legislation to implement Do-Not-Track, the FTC relied on voluntary efforts such as that by the W3C, an Internet standards setting organization. The FTC said Do-Not-Track must include five principles:

-- It should be implemented universally to cover all parties that would track consumers.
-- The choice mechanism should be easy to find, easy to understand and easy to use.
-- Any choice should be persistent and should not be overridden if cookies are cleared or the browser updated.
-- It should be comprehensive, effective and enforceable.
-- It should go beyond simply opting consumers out of receiving target advertisements; it should opt them out of collection of behavioral data for all purposes other than those

consistent with the context of the interaction. (For example preventing fraud or de-identified data for analytics).

Last week FTC Chairwoman Edith Ramirez told the American Federation of Advertisers:

> "Consumers still await an effective and functioning do-not-track system, which is now long overdue… An online advertising system that breeds consumer discomfort is not a foundation for sustained growth. More likely, it is an invitation to Congress and other policymakers in the U.S. and abroad to intervene with legislation or regulation and for technical measures by browsers or others to limit tracking."

W3C's Tracking Protection Working Group has been attempting to draft two standards. One would specify how technically a Do-Not-Track message would be sent, while the second would cover the obligations of a website that receives the Do-Not-Track message.

The six public interest groups also called for legislation to implement the Consumer Privacy Bill of Rights announced last spring by the White House. The Department of Commerce's National Telecommunications and Information Administration is running a "multi-stakeholder" process to develop a code to implement transparency about data use by mobile apps.

"The pace with both reaching a DNT standard and agreeing on an apps code has been glacial," said John M. Simpson, Consumer Watchdog's Privacy Project director. "We need to see the big stick of legislation. It's the only way to drive anything forward on either front."

"Consumers are increasingly powerless to stop the growing surveillance by marketers who follow their every click and action, whether they are online or using a mobile phone," said Jeff Chester, executive director of the Center for Digital Democracy. "It's time Congress protected the privacy of Americans by giving an individual the right to decide who may harvest their personal information."

"Consumers have repeatedly said that they do not want to be followed online and value their online privacy. Despite this, many companies have ignored their desire for more control over data tracking, collection, and sharing. In the face of consumer demand, advertisers and others have actively said they will not honor a DNT signal," said Michelle De Mooy, senior associate at Consumer Action. "We believe this is anti-consumer and anti-business. We are pleased that Congress isn't looking away, but taking a step in the right direction to protect consumer control and preference tools. This legislation gives consumers the control they need and deserve."

"Do-Not-Track mechanisms provide crucial balance between individuals' fundamental privacy interests and corporate interests, but they will only be effective if companies are required to respect the Do-Not-Track requests that they transmit, " said Susan Grant, director of consumer protection at Consumer Federation of America. "This legislation

will ensure that individuals will have tools that will actually work to protect them from unwanted tracking."

"Leaving the trackers in charge of Do-Not-Track worked well for powerful special interests, but not for consumers," said Ed Mierzwinski, U.S. PIRG Consumer Program Director. "Now it's time for Congress to establish enforceable, strong Do-Not-Track rights with 'on' as the default setting."

In another privacy-friendly development, Mozilla, the developer of the Firefox web browser, has announced it will by default block cookies from sites not visited by the user in a new version of its browser, expected to be released this summer. Cookies are little bits of computer code that allow a user to be tracked. Apple's Safari browser already blocks Third Party cookies from sites not visited. Google paid a $22.5 million penalty to the FTC for hacking past the privacy settings on Safari, which is used on iPhones and iPads and other Apple devices.

-30-

For information about the groups visit their websites:

The Center for Digital Democracy: http://www.democraticmedia.org/

Consumer Action: http://www.consumer-action.org/

Consumer Federation of America: http://www.consumerfed.org/

Consumer Watchdog: http://www.consumerwatchdog.org

Privacy Rights Clearinghouse: http://www.privacyrights.org/

U.S. PIRG: http://www.uspirg.org/