NOVEMBER / DECEMBER 2011

alec.org

INSIDE ALEC

A PUBLICATION OF THE AMERICAN LEGISLATIVE EXCHANGE COUNCIL

SPECIAL ISSUE

INTERNATIONAL RELATIONS +

TELECOMMUNICATIONS & INFORMATION TECHNOLOGY

Promoting U.S. Competitiveness through 21st Century Trade Agreements

By Gina Vetere

In a Battle Over Internet Taxes, Both Sides Invoke States' Rights

By Steve DelBianco

ALEC Alumni Spotlight

By U.S. Rep. Tom Graves (GA)

Protecting Consumer Privacy Requires a Steady Head and Steady Hand

BY BARTLETT CLELAND AND REP. BLAIR THORESON (ND)

Privacy in the digital world, citizen and consumer, is one of the important public policy issues of the 21st century. Users of technology want tools that provide great service and that work with ease and efficiency, but they don't necessarily want their lives tracked by marketers or government without their knowledge and consent, their email plagued with spam, or to necessarily have their social media information automatically made available to everyone on the network. And nobody wants their credit information exposed without their express consent.

State and federal legislators are struggling with the proper balance of consumer and citizen protection on the one hand and economic growth and government efficiency on the other. The combination of the explosive growth in the use of the Internet, the advent of social networking like Facebook and Twitter, and the spread of the mobile Internet has connected scores of people like never before, in ways inconceivable not long ago. Combine this rapid growth with consumers' sudden desire to be anonymous and "privacy" is one of the most challenging issue facing policymakers.

One reason why privacy is such a challenge for policymakers is because the concept is so difficult to define. Does it really mean "privacy" or "anonymity" or "confidentiality" or even something else.

Even different cultures and social groups have different understandings about the meaning of privacy based on their traditions and experiences.

In addition, our ability to seclude either ourselves or information about ourselves from others has been altered in many ways, some of which we do not yet fully understand, due to rapidly-changing technologies. That trend will only continue, and this causes fear in many.

Uninformed media-spun hyperbole about "invasions of privacy" that restrict freedom and assert Orwellian-style control make matters worse. Public opinion surveys by a variety of organizations show that vast majorities of Americans are concerned about online privacy.

While concerns about privacy are understandable, those concerns are not an excuse for hasty policymaking. Regrettably, policymakers' reaction to increased public concerns about privacy has been to introduce legislation or pursue regulations that ultimately can cause more problems than they will remedy.

At least half-a-dozen bills related to privacy, including a "Do Not Track bill" that would require express consent for all website tracking (even for basic usage information), are pending in Congress. Additionally, there have been several Congressional hearings on the topic of privacy and individual Members of Congress have called on regulators to investigate invasions of privacy. In the states, legislators and regulators from California to Indiana to Puerto Rico are trying to address concerns about privacy with their own laws and rules. In California, for example, legislators introduced two bills – SB242, *The Social Networking Privacy Act*, and SB761, a Do Not Track bill – to address recent concerns about privacy.

That is not to say that people should not be able to protect their privacy. In fact, as active participants in the digital world, we value privacy for ourselves. But much of the "privacy" legislation and regulations being proposed are unworkable and ultimately detrimental to the digital world. A more thoughtful approach to policymaking about privacy is critical.

Recently proposed laws raise a number of significant compliance, economic, and constitutional problems that should concern the private sector and policymakers. For example, how exactly would the identity verification system work? Such systems are not currently widely available due to technological hurdles and high costs. Additionally, restrictions to prevent adolescents from going online could lead to increased incidence of rule-breaking among teenagers as they engage in deception and devise other ways to evade the restrictions, thereby rendering them useless. Policymakers must think about what is workable, not just that which is politically expedient.

The Social Networking Privacy Act would mandate privacy by requiring social networking sites like Facebook and MySpace to take down personal information at the request of users or the parents of users under 18 years of age. Similarly, the Do Not Track (DNT) bill, as its name suggests, would require an opt-out for any

data collection from visitors to a website. The regulations necessary to fulfill these mandates would likely mean a system of identity verification for all social network users and a new technology added to all websites and a possible government registry.

A DNT scheme would seriously jeopardize the substantial and growing digital economy, and consumers' ability to obtain goods at services online at no or low cost. Many of the "free" services, such as e-mail, search, and even news that consumers use and depend on are of no-cost to them because advertisers subsidize the websites we use. In exchange, advertisers collect data on where we go and what we do to design and target advertising for companies. But DNT would prevent this arrangement on a wide scale, thus forcing consumers to have to pay for the services.

"Market-based solutions to privacy concerns should continue."

Introducing new costs into the digital economy could seriously hamper economic growth and job creation, especially among small and new businesses. A recent study by the Massachusetts Institute of Technology and the University of Toronto compared the purchase intentions of 3.3 million individuals across five European Union (EU) and five non-EU countries over the eight-year period after EU nations began implementing opt-in requirements to follow the European's DNT Privacy Directive, the most stringent privacy mandate in the world and the model for the DNT idea in the United States.[1]

What the study found was that "after the Privacy Directive was passed, advertising effectiveness decreased on average by around 65 percent in Europe relative to the rest of the world."[2] This is to say that individuals received a vastly higher percentage of completely irrelevant information to them. Net Choice, a trade association representing e-commerce and Internet companies, estimates that an EU-style "opt-in" requirement could cost U.S. companies $33 billion over five years.[3] While large companies might be able absorb these new regulatory and compliance costs, smaller companies and startups, one of the few bright spots in the economy, could be forced to shut down or flee.

Constitutional jurisdiction is another potential problem. Because virtually all aspects of the digital world are interstate, these laws could be challenged in court on interstate commerce grounds with unpredictable consequences for the state's legislative and regulatory structures.

Rather than problematic and unrealistic mandates, what consumers and policymakers really need to help ensure better protection of privacy is continued education and transparency by internet service providers, social networks, and website owners on how their information is collected and used.

There are tremendous efforts on this front underway. Dynamic market forces have encouraged companies to alter how they collect and use information. Online markets have responded very quickly to consumers' concerns about privacy. Companies like Facebook, Google, and Microsoft have published more thoroughly-developed guidelines and made available easy-to-use tools enabling users to better control their information. Apple changed how it collects geo-location data, not because of a government mandate, but because the public expressed its concern directly to the company. Market-based solutions to privacy concerns should continue.

Moreover, it may be worth considering how we think about privacy and how that value interacts with our other cherished American values about limited government and individual liberty that ALEC members hold dear. Adam Thierer, a senior research fellow at the Mercatus Center at George Mason University, has written that "a good case can be made for restraint when it comes to legislating to define and protect privacy. That doesn't mean privacy isn't important—it is. But how we go about 'protecting' it needs to be balanced against other rights and responsibilities."[4]

This is a conversation we look forward to having here at ALEC and in our professional lives.

BARTLETT CLELAND is Policy Counsel with the Institute for Policy Innovation. **REP. THORESON** represents District 44 in the North Dakota House of Representatives. Respectively, they are the private and public sector co-chairs of ALEC's Telecommunications & Information Technology Task Force.

[1] http://www.netchoice.org/library/estimate-of-us-revenue-loss-if-congress-mandated-opt-in-for-interest-based-ads/

[2,3] Ibid.

[4] http://www.forbes.com/sites/adamthierer/2011/09/25/is-privacy-overrated/2/