POLITICO

Privacy lines drawn over president's cyber map

December 17, 2013
By: Tony Romm

An Obama administration plan to improve the country's digital defenses has become a makeshift privacy battlefield.

A draft set of cybersecurity best practices commissioned by the president and authored alongside industry prescribes that power plants, financial institutions and others should secure their systems by limiting their collection and storage of sensitive customer information — the very data often in hackers' crosshairs.

The language, however, only has served to pit privacy hawks who seek better consumer protections against industries that have long lobbied Washington against any new mandates.

Electric utilities and their trade groups, business lobbies like the U.S. Chamber, tech giants including Microsoft, and major contractors like Honeywell have urged the government to stand down. In vague terms, these companies and trade organizations have hinted industry might not back the administration's final plan in full if it includes broad, new privacy rules — a claim that's since stirred civil-liberties leaders at the ACLU and others to action.

"Protecting privacy is necessary for the public to feel confident in continuing to engage with new and developing technology; and cybersecurity initiatives should make protecting that privacy a paramount goal," privacy hawks wrote.

For now, the federal agency that's leading the process to write those guidelines has remained quiet. A spokeswoman for the National Institute of Standards and Technology declined comment for this story. A final draft of the cybersecurity framework is due next year.

The Beltway's biggest lobbying shops for years have fought successfully against any new comprehensive digital privacy law. And, in a sense, cybersecurity has suffered a similar fate: Corporate lobbying also derailed any hopes for comprehensive cybersecurity reform last year, though Obama in February signed an executive order that now has government and industry working together on best practices.

The framework is voluntary: Companies can choose to adopt it, and they may be awarded by the federal government if they do. While the effort has won notable, early praise, big

businesses still are taking great exception to an appendix of the draft framework that calls on companies to better safeguard their warehouses of personal information.

Specifically, the administration's blueprint urges industry to identify the personally identifiable data in its control, and offer customers notice and choice about how that data is used. So too does the draft emphasize that companies "limit the use and disclosure" of that data, while making things as anonymous as possible.

Yet it's not sitting well with industry, including a collection of major energy providers that explicitly criticized the section this month. Writing in public comments, the American Gas Association, Edison Electric Institute, the Utilities Telecom Council and others fretted the framework included "independent privacy protections unrelated to the protection of critical infrastructure."

Reacting quickly in public comments, the U.S. Chamber called it "troubling" and urged the administration to make clear it's not trying to "establish broader privacy requirements for industry." Honeywell asked NIST to consider something more "narrowly focused." Microsoft predicted it would "create unnecessary, onerous compliance costs and risk discouraging organizational adoption" of the voluntary best practices. And TechAmerica argued "the cybersecurity framework is not the appropriate time or place to attempt to make privacy policy beyond what is necessary for cybersecurity."

Privacy groups are trying to ward off any change. The ACLU joined the Center for Democracy and Technology, The Constitution Project, the Electronic Frontier Foundation and others in supportive comments filed Friday. "While we believe that some flexibility is warranted, we urge NIST to reject the invitation that it water down the role of FIPPs in the framework," they wrote.

Still, many critics — including the Chamber, Microsoft and TechAmerica — instead recommended a rewrite submitted by Harriet Pearson, a partner with Hogan Lovells. Her suggestion, drafted with unnamed industry input, is a significantly pared down privacy section that mostly emphasizes the need for companies to have processes in place to assess their privacy practices as they swap cyberthreat data and scan their systems. For their part, civil-liberties hawks blasted Pearson's work product in a footnote of their public filing.