TWO THEMES FROM OBAMA'S CYBERSECURITY PROPOSAL: PRIVATE AUDITORS AND IMMUNITY

Two and a half years after privatized auditors largely signed off on practices that contributed to the collapse of Wall Street, and a year after coziness between government inspectors and the oil industry they regulate allowed a massive oil spill in the gulf, the Obama Administration proposes relying on private auditors to ensure that private companies guard our nation's cybersecurity.

That's one of two troubling aspects of the fact sheet the Administration just released, summarizing proposed legislation on cybersecurity it just sent to Congress.

At issue is who investigates the adequacy of a private companies' cybersecurity plan to both certify it is adequate and ensure compliance with it. The answer? Auditors paid by the private companies.

> The Administration proposal requires DHS to work with industry to identify the core critical-infrastructure operators and to prioritize the most important cyber threats and vulnerabilities for those operators. Critical infrastructure operators would develop their own frameworks for addressing cyber threats. Then, each critical-infrastructure operator would have a third-party, commercial auditor assess its cybersecurity risk mitigation plans. Operators who are already required to report to the Security and Exchange Commission would also have to certify

> that their plans are sufficient. A summary of the plan would be accessible, in order to facilitate transparency and to ensure that the plan is adequate. In the event that the process fails to produce strong frameworks, DHS, working with the National Institute of Standards and Technology, could modify a framework. DHS can also work with firms to help them shore up plans that are deemed insufficient by commercial auditors.

While the promise to make these plans transparent is all well and good, the problem remains that private companies and the auditors they pay get to decide what is sufficient, not someone without a financial stake in the outcome. If government inspectors are important enough for safety issues, shouldn't they be required for the cyberinfrastructure that is so critical to our safety?

In addition, a big part of this plan may give up one of the sticks the government has to ensure compliance.

One of the reasons why private companies don't like to reveal when they've been hacked is liability issues: not only might their customers respond badly, but in some fields (like finance companies) the companies may face other liability issues.

But the fact sheet offers companies immunity, at the least, for any private data it shares with the government when it reveals it has been hacked.

> Voluntary Information Sharing with Industry, States, and Local Government. Businesses, states, and local governments sometimes identify new types of computer viruses or other cyber threats or incidents, but they are uncertain about whether they can share this information with the Federal

> Government. The Administration proposal makes clear that these entities can share information about cyber threats or incidents with DHS. To fully address these entities' concerns, it provides them with immunity when sharing cybersecurity information with DHS. At the same time, the proposal mandates robust privacy oversight to ensure that the voluntarily shared information does not impinge on individual privacy and civil liberties.

The fact sheet doesn't describe the extent of the immunity, and the plan does, at least, make immunity contingent upon privacy protections.

- When a private-sector business, state, or local government wants to share information with DHS, it must first make reasonable efforts to remove identifying information unrelated to cybersecurity threats.

> [snip]

- Immunity for the private-sector business, state, or local government is conditioned on its compliance with the requirements of the proposal.

But I wonder about the breadth of this immunity. Does it also offer companies immunity for negligence in the handling of consumer data?

One thing that Al Franken, among others, is

pushing, is making it easier for consumers to expect a certain level of protection for their data. Thus, if Sony has two-year-old consumer data sitting around in an unsecure server, it would bear some liability if a hacker came and access that data. Such measures would effectively expose companies to lawsuit if they totally blew off their customers' data security.

Now at least this proposal mandates that companies tell consumers when their data has been accessed (though I always worry when federal legislation claims to simplify state legislation—it's often code for "water down").

> National Data Breach Reporting. State laws have helped consumers protect themselves against identity theft while also incentivizing businesses to have better cybersecurity, thus helping to stem the tide of identity theft. These laws require businesses that have suffered an intrusion to notify consumers if the intruder had access to the consumers' personal information. The Administration proposal helps businesses by simplifying and standardizing the existing patchwork of 47 state laws that contain these requirements.

But it's not clear whether companies would bear any liability for such breaches if and when they alert consumers. Moreover, this says nothing about other public disclosure on breaches, which consumers may have as big an interest in (for example, investors ought to be able to know if banks and other major investors routinely get hacked, and stock holders ought to be able to know if critical proprietary information has been stolen).

Call me crazy, but my hackles start to rise when the government starts granting immunity willy nilly, with almost nothing demanded in exchange.

Update: Kashmir Hill offers one example why a national "simplified" law might be a

problem—because it’ll eliminate elements like mandatory identity theft protection and penalties from the most stringent law, in MA.

> As for telling customers about their data being breached, the White House says it will “help businesses” by simplifying and standardizing the “existing patchwork of 47 state laws” that have various requirements about how soon to notify customers. In the fact sheet, at least, there’s no mention of penalties for businesses, nor mandatory provision of identity theft monitoring after a breach — two aspects of the harshest data breach law currently in the country, in Massachusetts.