The Heritage Foundation
LEADERSHIP FOR AMERICA

ISSUE BRIEF

No. 4032 | SEPTEMBER 3, 2013

How Obamacare Threatens Privacy in America

Chris Jacobs

Over the past several months, a stream of reports from government auditors and news stories has raised serious questions about the Administration's implementation of Obamacare and its effects on the privacy of millions of Americans. The reports paint a portrait of an Administration casting aside security concerns—potentially putting Americans' financial and health data at risk—in its push to open insurance exchanges in all 50 states by October 1. These recent developments should provide further impetus for Congress to defund the entire law before the exchanges are able to undermine personal privacy.

Security Delays, Timetables Slipping. In August, the Department of Health and Human Services (HHS) inspector general released a report highlighting many missed deadlines with respect to the security measures surrounding the Obamacare data hub.[1] The hub will provide access to government data from various government agencies—tax filings and Social Security records, for example—allowing exchanges to determine eligibility for subsidized insurance.

The inspector general's report found that "several critical tasks remain to be completed in a short period of time" in order to ensure the data hub's security.[2] Important elements of the security testing were delayed by two months. As a result, the official certification that the data hub is secure is not scheduled to occur until September 30, 2013—one day before the exchanges are scheduled to open for business.[3]

The inspector general's report noted the obvious problem that this tight timetable presents: "If there are additional delays...the authorizing official may not have the full assessment of implemented security controls needed for the security authorization decision by" the time open enrollment begins.[4] In other words, government officials could face a choice about whether to open the exchanges despite the potential risk to Americans' data security. Even if the security assessments are completed on time, there is no assurance they will work properly; the inspector general's report "did not review the functionality of the [data] hub."[5]

Warnings Ignored. Some government officials have warned of the privacy and security implications arising from shoddy data security—even as the Obama Administration ignored those concerns. Michael Astrue, a former general counsel of HHS, offered objections while serving as the commissioner of Social Security through February 2013. He has called the Administration's exchange portal "an overly simplistic system without adequate privacy safeguards":

> The system's lack of any substantial verification of the user would leave members of the public open to identity theft, lost periods of health insurance coverage, and exposure of address for victims of domestic abuse and others.[6]

This paper, in its entirety, can be found at
http://report.heritage.org/ib4032

Produced by the Center for Health Policy Studies

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

Astrue dubbed the version of the portal "the most widespread violation of the Privacy Act in our history," noting that both he and the head of the IRS "raised strong legal objections" with the Office of Management and Budget—objections that, Astrue argues, have been ignored in favor of what he calls "an absurdly broad interpretation of the Privacy Act's 'routine use' exemption."[7]

Navigators Pose a Security Risk. While the data hub creates concerns that Americans could be subjected to electronic identity fraud, Obamacare's "navigators" could subject Americans to in-person scams.[8] HHS recently announced it was lowering by one-third—from 30 hours to 20—the minimum training time for navigators.[9] As a result, individuals can be certified as navigators with fewer than three full days' training—and few security checks. While guidelines regarding navigators released in July permitted states to establish "minimum eligibility criteria and background checks" for navigators, it did not require them to do so.[10]

Because their job involves helping Americans figure out their insurance options, navigators will often have access to sensitive personal information—bank accounts, Social Security numbers, insurance identification, and more. Yet navigators will not be required to undergo background checks, and the process for filing complaints about unscrupulous navigators remains unclear at best. Even California's insurance commissioner—a Democrat and strong supporter of Obamacare—raised concerns that navigators would put consumers at risk for scams: "We can have a real disaster on our hands."[11]

Not One Dime. Federal agencies have already encountered difficulties preserving the integrity of Americans' sensitive information. Earlier this year, a medical provider in California sued the IRS for improperly seizing 60 million records of 10 million Americans.[12] Yet under Obamacare, the IRS and other federal agencies will hold more new powers and have access to even more of Americans' personal health and financial information.

In its mad rush to implement its unworkable law, the Obama Administration has taken a slapdash and shoddy approach to Americans' personal security. Given these stakes, the choice for Congress could not be clearer: Congress should preserve Americans' privacy by refusing to spend another dime implementing Obamacare.

*—**Chris Jacobs** is Senior Policy Analyst in the Center for Health Policy Studies at The Heritage Foundation.*

1. Gloria Jarmon, "Memorandum Report: Observations Noted During the OIG's Review of CMS's Implementation of the Health Insurance Exchange—Data Services Hub," Department of Health and Human Services Inspector General *Report* A-18-13-30070, August 2, 2013, http://oig.hhs.gov/oas/reports/region1/181330070.pdf (accessed August 29, 2013).
2. Ibid., p. 1.
3. Ibid., p. 5.
4. Ibid., p. 5.
5. Ibid., p. 2.
6. Michael Astrue, "Privacy Be Damned," *The Weekly Standard*, August 5, 2013, http://www.weeklystandard.com/articles/privacy-be-damned_741033.html (accessed August 29, 2013).
7. Ibid.
8. For more information on the navigator program, see Alyene Senger, "The Cost of Educating the Public on Obamacare," Heritage Foundation *Issue Brief* No. 3983, July 1, 2013, http://www.heritage.org/research/reports/2013/07/public-outreach-on-obamacare-cost-of-educating-the-public-on-health-care-reform.
9. Amy Schatz, "Preparations for Health Exchanges on Tight Schedule," *The Wall Street Journal*, August 7, 2013, http://online.wsj.com/article/SB10001424127887324170004578638100820728288.html (accessed August 29, 2013).
10. "Department of Health and Human Services: Patient Protection and Affordable Care Act; Exchange Functions: Standards for Navigators and Non-Navigator Assistance Personnel; Consumer Assistance Tools and Programs of an Exchange and Certified Application Counselors; Final Rule," *Federal Register*, Vol. 78, No. 137 (July 17, 2013), p. 42824, http://www.gpo.gov/fdsys/pkg/FR-2013-07-17/pdf/2013-17125.pdf (accessed August 29, 2013).
11. "Fraud Fear Raised in California's Health Exchange," *The Reporter*, July 14, 2013, http://www.thereporter.com/rss/ci_23658245 (accessed August 29, 2013).
12. Scott Gottlieb, "Suit Alleges IRS Improperly Seized 60 Million Personal Medical Records," Forbes, May 15, 2013, http://www.forbes.com/sites/scottgottlieb/2013/05/15/the-irs-raids-60-million-personal-medical-records/ (accessed August 29, 2013).