**U.S. HOUSE OF REPRESENTATIVES**
**COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY**
**SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY**
**SUBCOMMITTEE ON OVERSIGHT**

***Can Americans Trust the Privacy and Security of their Information on HealthCare.gov?***

**Thursday, February 12, 2015**
**2:00 p.m. – 4:00 p.m.**
**2318 Rayburn House Office Building**

## Purpose

On Thursday, February 12, 2015, the Research and Technology Subcommittee and the Oversight Subcommittee will hold a joint hearing titled *Can Americans Trust the Privacy and Security of their Information on HealthCare.gov?* The hearing stems from recent news reports[1] that dozens of data firms have embedded connections on HealthCare.gov, and that through these connections, the companies could potentially collect and sell personal health, financial, and other information from citizens through the HealthCare.gov website. The hearing will examine both the privacy implications to consumers' personal information from the presence of the companies connected to HealthCare.gov, and whether these third party connections add vulnerabilities to the website's security.

A broader question related to the hearing is why the U.S. government would allow data-mining companies such open access to such personal data flowing through HealthCare.gov or any government website. Given the President's Executive Order on Open Data issued in May 2013 calling for departments and agencies of the federal government to be "more accessible to the public and to entrepreneurs,"[2] was it also properly communicated that the government should also take steps "appropriately safeguarding sensitive information and rigorously protecting privacy"?[3]

## Witnesses

- **Ms. Michelle De Mooy**, Deputy Director, Consumer Privacy, Center for Democracy and Technology
- **Mr. Morgan Wright**, Principal, Morgan Wright, LLC

## Overview

On January 20, 2015, the *Associated Press* reported that when consumers "apply for coverage on HealthCare.gov, dozens of data companies may be able to tell that you are on the site. Some can even glean details such as your age, income, ZIP code, whether you smoke or if you are pregnant."[4] The news report identifies "50 third-party connections embedded on HealthCare.gov,"[5] and quotes a staff

---

[1] Ricardo Alonzo-Zaldivar and Jake Gillum, "New Privacy Concerns Over Government's Health Care Website," *Associated Press*, January 20, 2015, available at: http://apnews.myway.com/article/20150120/us--health_overhaul-privacy-8b7c5d925b.html; hereinafter AP News Report.
[2] OSTP Initiatives, available at: http://www.whitehouse.gov/administration/eop/ostp/initiatives#Openness; hereinafter OSTP Initiatives.
[3] Ibid.
[4] AP News Report, *supra*, note 1.
[5] Ibid.

technologist from the Electronic Frontier Foundation, a civil liberties group, as saying, "Third-party embedded websites are troubling because they can be used to track you and track your reading when you're browsing the Web."[6]

In addition to these privacy concerns, the presence of the high number of embedded connections on HealthCare.gov also raises security concerns, because, as one cybersecurity expert explained, "As I look at vendors on a website...they could be another potential point of failure."[7] Ms. Cheri McGuire, vice-president of cybersecurity policy for Symantec Corporation, echoed similar concerns during a hearing last month before the Subcommittee on Research and Technology when she noted, in response to a question, that opening up HealthCare.gov to so many embedded third parties created additional vulnerabilities.[8]

While a CMS spokesman defended the practice by claiming that "outside vendors 'are prohibited from using information from these tools on HealthCare.gov for their companies' purposes,'"[9] the Administration "did not explain how it ensures that privacy and security policies are being followed."[10]

Since the *AP*'s report last month, private cybersecurity experts, online privacy advocates, and the House Energy & Commerce Committee[11] have also confirmed that HealthCare.gov has facilitated embedded connections for data companies that enable them to receive the website users' personal and health care information automatically.

**Background**

*FISMA*

The data on HealthCare.gov is one of the largest collections of personal information ever assembled, linking information from seven different federal agencies along with state agencies and government contractors. Federal agencies have a duty to ensure that these private records have sufficient protection from misuse and security breaches under the Federal Information Security Management Act of 2002 (FISMA), which requires all federal agencies to develop and implement programs that secure their information and information systems.

The National Institute of Standards and Technology (NIST), "develops and issues standards, guidelines, and other publications to assist federal agencies in implementing FISMA and in managing cost-effective programs to protect their information and information systems."[12] Each agency's information control system must be reviewed, certified and accredited under NIST publication SP 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems."[13] Security

---

[6] Ibid.
[7] Ibid.
[8] House Science, Space, and Technology Subcommittee on Research and Technology hearing, "The Expanding Cyber Threat," January 27, 2015, available at: http://science.house.gov/hearing/subcommittee-research-and-technology-hearing-expanding-cyber-threat; hereinafter Research and Technology Subcommittee Hearing.
[9] AP News Report, *supra*, note 1.
[10] Ibid.
[11] House Energy and Commerce Committee, "House and Senate Committee Leaders Press Administration on HealthCare.gov Security," January 30, 2015, available at: http://energycommerce.house.gov/press-release/house-and-senate-committee-leaders-press-administration-healthcaregov-security.
[12] NIST, Information Technology Laboratory, Computer Security Division, Computer Security Resource Center, FISMA Compliance, available at: http://csrc.nist.gov/groups/SMA/fisma/compliance.html.
[13] NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems," May 2004, available at: https://www.fismacenter.com/SP800-37-final.pdf.

accreditation is required under OMB Circular A-130, Appendix III. Accredited systems must be monitored continuously, including ongoing assessment of security controls. By accrediting an agency's information system, the responsible agency official "accepts responsibility for the security of the system and is fully *accountable* for any adverse impacts to the agency if a breach of security occurs."[14]

Under FISMA, the Director of the Office of Management and Budget (OMB) is required to oversee the information security policies and practices of federal agencies, which include "assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems."[15]

*NIST Cybersecurity Framework*

In February 2013, President Obama issued Executive Order 13636 on cybersecurity for critical infrastructure, which states that it is "the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."[16]

The Executive Order describes critical infrastructure as, "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[17] The Executive Order also directed NIST to "lead the development of a framework to reduce cyber risks to critical infrastructure,"[18] and in February 2014, NIST released the *Framework for Improving Critical Infrastructure Cybersecurity*[19] (Framework).

NIST worked in collaboration with industry stakeholders to establish this three-pronged document that includes a Core, Profile and Implementation Tiers. "The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure."[20] The Framework also assists "organizations in incorporating privacy and civil liberties as part of a comprehensive cybersecurity program."[21] During the Research and Technology Subcommittee hearing previously referenced, another witness, Dr. Charles Romine from NIST, noted in response to a question that the Framework "does have a pretty strong statement to say about privacy, and NIST has embarked on a privacy engineering research activity partly as a result of what we learned from the framework process, that there needs to be more guidance and more tools available for people to promote privacy considerations."[22]

---

[14] Ibid; (Emphasis in original).
[15] Public Law 107-347, available at: http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf
[16] Executive Order – Improving Critical Infrastructure Cybersecurity, February 12, 2013, available at: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.
[17] Ibid.
[18] Ibid.
[19] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.0, February 12, 2014, available at: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.
[20] Ibid.
[21] Ibid.
[22] Research and Technology Subcommittee Hearing, *supra*, note 8.

*Government Reports*

Various reports issued in the past few months by federal watchdog agencies have identified privacy and security concerns about HealthCare.gov. For example, a GAO report from last fall identified weaknesses "in the processes used for managing information security and privacy as well as the technical implementation of IT security controls."[23] More recently, a report[24] from the U.S. Department of Health and Human Services' Office of Inspector General revealed contract planning and procurement failures, which also raises questions about the ability of HealthCare.gov to protect consumers' private and sensitive information.

*Health Care Breaches*

Last September, news organizations reported that a "hacker broke into part of the HealthCare.gov insurance enrollment website in July and uploaded malicious software."[25] And as recently as last week, consumers learned about what is being described as perhaps the largest data breach against a health care company when Anthem Inc., the country's second-biggest health insurer, was attacked. Anthem disclosed that "names, birth dates, Social Security numbers, medical IDs, street and e-mail addresses and employee information including income levels were stolen"[26] for 80 million Anthem members. This has prompted the suggestion that consumers should closely monitor their medical statements because medical or "health-insurance information can sell for 10 times what a credit card number fetches on the black market, making it a lucrative area for cybercriminals."[27]

*Open Data Policy*

The broader question is why the Administration decided to share such private consumer data from American citizens who were required to register for HealthCare.gov. On May 9, 2013, the Administration issued a memorandum on open data policy noting that, "Information is a valuable national resource and a strategic asset to the Federal Government, its partners, and the public. In order to ensure that the Federal Government is taking full advantage of its information resources, executive departments and agencies…must manage information as an asset throughout its life cycle to promote openness and interoperability, and properly safeguard systems and information."[28]

The President also issued an Executive Order the same day to establish an Open Data Policy to make "open and machine-readable data the new default for government information, taking historic steps

---

[23] U.S. Government Accountability Office, "HealthCare.gov: Actions Needed to Address Weaknesses in Information Security and Privacy Controls, Report GAO-14-730, September 2014, available at: http://www.gao.gov/assets/670/665840.pdf.

[24] U.S. Department of Health and Human Services, Office of Inspector General, "Federal Marketplace: Inadequacies in Contract Planning and Procurement," Report OEI-03-14-00230, January 2015, available at: https://oig.hhs.gov/oei/reports/oei-03-14-00230.pdf.

[25] Danny Yadron, "Hacker Breached HealthCare.gov Insurance Site," *The Wall Street Journal*, September 4, 2014, available at: http://online.wsj.com/articles/hacker-breached-healthcare-gov-insurance-site-1409861043.

[26] Shannon Pettypiece, "What to do Right Now If You're One of the 80 Million Anthem Members Who Got Hacked," *Bloomberg*, February 5, 2015, available at: http://finance.yahoo.com/news/now-youre-one-80-million-214043538.html;_ylt=A0LEVv1K4tZU124ALt0nnIlQ.

[27] Ibid.

[28] Office of Management and Budget Memorandum (M-13-13), From Sylvia Burwell, OMB Director, Steven VanRoekel, Federal Chief Information Officer, Todd Park, U.S. Chief Technology Officer and Dominic J. Mancini, Acting Administrator, Office of Information and Regulatory Affairs, May 9, 2013, available at: http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf.

to make government-held data more accessible to the public and to entrepreneurs while appropriately safeguarding sensitive information and rigorously protecting privacy."[29] This situation with HealthCare.gov seems to indicate that the Administration was more interested in providing government-held data to entrepreneurs for the purposes of data-mining than in protecting privacy.

However, an interim progress report released last week, spearheaded by John Podesta, counselor to the President, raises serious privacy concerns related to big data technologies. In response to a request from President Obama for a "wide-ranging review of big data and privacy,"[30] the report notes:

> "While there are promising technological means to better protect privacy in a big data world, the report's authors concluded these methods are far from perfect, and technology alone cannot protect privacy absent strong social norms and a responsive policy and legal framework. Finally, the report raised issues around other values potentially implicated by big data technology—particularly with regard to the potential for big data technologies to lead, purposely or inadvertently, to discriminatory outcomes on the basis of race, gender, socioeconomic status, or other categories."[31]

In a parallel effort, the Podesta report was supported by the President's Council of Advisors on Science and Technology (PCAST) "to investigate the scientific and technological dimensions of big data and privacy."[32] In a report issued last year, the Council notes:

> "The challenges to privacy arise because technologies collect so much data (e.g., from sensors in everything from phones to parking lots) and analyze them so efficiently (e.g., through data mining and other kinds of analytics) that it is possible to learn far more than most people had anticipated or can anticipate given continuing progress. These challenges are compounded by limitations on traditional technologies used to protect privacy (such as de-identification). PCAST concludes that technology alone cannot protect privacy, and policy intended to protect privacy needs to reflect what is (and is not) technologically feasible."[33]

Against this backdrop, the hearing will examine the privacy and cybersecurity questions raised by the embedded connections of dozens of third party data firms on HealthCare.gov.

---

[29] OSTP Initiatives, *supra*, note 2.

[30] John Podesta, Counselor to the President, Penny Pritzker, Dept. of Commerce Secretary, Ernest Moniz, Dept. of Energy Secretary, John Holdren, OSTP Director, Jeff Zients, Economic Advisor to the President, Interim Progress Report, "Big Data: Seizing Opportunities, Preserving Values," February 2015, available at: http://www.whitehouse.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf..

[31] Ibid.

[32] Ibid.

[33] PCAST Report to the President, "Big Data and Privacy: A Technological Perspective," May 2014, available at: http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.