Bloomberg BNA

Privacy & Security Law Report®

VOL. 13, NO. 17 APRIL 28, 2014

Internet

Lack of Privacy, Security Might Hinder Future of Internet of Things, Speakers Say

The lack of privacy and security could be a major disabler for the Internet of things (IoT), speakers said April 24 at the 2014 Association of National Advertisers Advertising Law & Public Policy Conference.

The IoT involves the ability of physical objects to connect to the Internet.

Risks to the privacy and security of data are some of the ''greatest threats'' to the IoT, Christin McMeley, a partner at Davis Wright Tremaine LLP in Washington, said. The complexity of the IoT in combination with the volume of data involved creates new issues and risks, she said.

The ''threat landscape'' hasn't changed very much, but the opportunities for data compromise have ''increased significantly,'' John Ciesla, global director of information security for marketing and advertising agency Grey Group in New York, said.

Enablers and Disablers. One of the things that has enabled the IoT to develop is the transition from the Internet protocol known as IPv4 to an Internet protocol called IPv6, Ciesla said. IPv6 has provided more IP addresses and more efficiencies, Ciesla said.

Besides technology, the business-driven nature of IoT and the cost savings that it offers have also enabled IoT, according to McMeley and Ciesla.

But there are also disablers for the IoT, they said. The lack of standards might be a ''big disabler,'' Ciesla said. Other potential disablers include the lack of bandwidth, government intervention and unanticipated costs, according to McMeley and Ciesla.

In addition, ''privacy and data security concerns abound,'' McMeley said. Privacy and security issues, along with the ''temptation to regulate in this area,'' might ''stifle innovation,'' she said.

Consumers May 'Turn Away.' Consumers have a ''fundamental trust'' that their information will be secured, McMeley said. If consumers cannot trust that their information will be protected, they may ''turn away,'' she said.

Legal challenges related to privacy and security, such as data breach lawsuits, can also be disablers, according to McMeley. Regulatory enforcement and the potential for significant fines are also drawbacks, she added.

The IoT has caught the attention of regulators. The U.S. Federal Trade Commission hosted a workshop on privacy and security issues related to the IoT in November 2013, at which speakers stressed the need for privacy by design in connected devices (12 PVLR 1980, 11/25/13) and FTC Chairwoman Edith Ramirez said core privacy principles should govern the IoT (12 PVLR 1979, 11/25/13).

In February, the European Commission published a report on the results of a public consultation on the IoT, McMeley pointed out.

The ''threat landscape'' hasn't changed very much, but the opportunities for data compromise have ''increased significantly.''

JOHN CIESLA, GLOBAL DIRECTOR OF INFORMATION SECURITY, GREY GROUP

The FTC announced in September 2013 that it had settled its first IoT case (12 PVLR 1532, 9/9/13). The commission alleged that TRENDnet Inc.'s lax security practices led to the online posting of live feeds from about 700 home surveillance cameras. The FTC Feb. 7 announced that it had finalized the consent order with TRENDnet (13 PVLR 289, 2/17/14).

Managing IoT Moving Forward. Given that advancements in Internet technology have increased the opportunities for the compromise of data, it is important that correct controls are implemented to protect data, Ciesla said. If the right controls aren't applied, exposure to threats becomes ''exponentially greater,'' he said.

Among the important goals of the IoT is to ''establish comprehensive data flows,'' according to McMeley and Ciesla.

''Know where your data is'' and ''how it's being treated within the system,'' Ciesla said.

Other important goals include privacy by design, de-identification, authentication and facilitating electronic discovery, McMeley said.

BY KATIE W. JOHNSON

 ISSN 1538-3423

To contact the reporter on this story: Katie W. Johnson in Washington at kjohnson@bna.com

To contact the editor responsible for this story: Donald G. Aplin at daplin@bna.com

Full text of the European Commission's ''Report on the Public Consultation on IoT Governance'' is available at http://op.bna.com/pl.nsf/r?Open=dapn-9jhmbn.

  PVLR ISSN 1538-3423