

# Who is Watching you Watch TV? If You Have VIZIO ... Your TV Might Be Watching You

February 13, 2017 | Blog | By [Cynthia J. Larose](#), Joanne Dynak

---

## VIEWPOINT TOPICS

- Privacy & Cybersecurity

---

## RELATED PRACTICES

---

## RELATED INDUSTRIES

What does your TV-watching history say about you? According to a recent lawsuit against VIZIO, Inc., it might be more than you think! One of the world's largest sellers of "smart" televisions **has recently paid a \$2.2 million settlement** following charges by the Federal Trade Commission and the Office of the New Jersey Attorney General that it was unlawfully tracking and selling 11 million consumers' viewing data. The resulting court order has important repercussions for both consumers and smart TV producers.

### Background

Beginning in February 2014, VIZIO, Inc. began manufacturing smart TVs (televisions with Internet connectivity). The company soon after launched a software update installing "Smart Interactivity," an automated content recognition feature that could conveniently make program recommendations based on your viewing history. This meant that VIZIO could collect detailed information about consumers' TV-watching habits on a second-by-second basis. Such viewing data was then coupled with the IP addresses of other Internet-enabled devices in a household to analyze consumer behavior – if an ad online led you to watch a show on TV, or if a commercial spurred you to check out a website, that activity was recorded. VIZIO used third parties to append specific demographic information to the viewing data, including sex, age, income, marital status, household size, education level, home ownership, and household value. The agencies alleged that VIZIO then sold this information to third parties who used it for various purposes, including targeting advertising to consumers across devices.

### Legal implications

According to the **complaint**, VIZIO failed to adequately inform its consumers that it would be tracking their viewing history and offering it to third parties. The software update enabling Smart Interactivity was preceded by a brief notification that the software was being installed and could be disabled in the settings; it did not explain up-front which data was being collected or with whom it would be shared. The complaint alleges that as a result of VIZIO's unfair and deceptive behavior, this data tracking was occurring without user consent, violating Section 5 of the FTC Act as well as New Jersey consumer protection statutes.

In addition to a \$1.5 million settlement payment to the FTC and \$1 million to the New Jersey Division of Consumer Affairs, **VIZIO was ordered** to delete all the data it has collected prior to March 1, 2016 (with certain exceptions) via Smart Interactivity and update its online and onscreen disclosures to accurately reflect its practices.

While the outcome of this case seems to address the legal problems with VIZIO's actions, the reasoning behind it may be subject to reconsideration. **In a concurring statement**, Acting FTC Chairman Maureen Ohlhausen examines Count I of the initial complaint, which alleged that the "granular" TV viewing data collected by VIZIO was "sensitive information", and that sharing this data without consent can cause "substantial injury" as defined by the FTC Act. Ohlhausen questions whether viewing data, and the potential harm associated with sharing it, should in fact be placed in the same category as other pieces of information the FTC defines as sensitive -- "financial information, health information, Social Security Numbers, information about children, and precise geolocation information." She cautions against conflating privacy rights with consumer protection against unfair practices, and wants the FTC to more precisely determine what constitutes "substantial injury" when it comes to consumer data.

### Looking forward: same problems, new technology

While VIZIO's actions and resulting lawsuit are alarming, they are not surprising. Americans are being **increasingly desensitized** to the widespread collection of personal data, be it from their Internet browsers, phone apps, social media profiles, or **voice-activated home systems**. While VIZIO's collecting

and combining data provide a strikingly comprehensive overview of the lives of its individual consumers, what got the company into legal trouble was the lack of effective notice before doing so. Other TV-makers have recently faced similar charges; **in 2015, Samsung landed in hot water** when it was revealed that its smart TVs' voice recognition system was capturing private home conversations and sharing the audio data with third parties. These cases raise critical questions about the trade-offs between the rapidly evolving capacity of technology, market competition, and the value of information about our personal lives.

## Authors

**Cynthia J. Larose**, Member / Co-chair, Privacy & Cybersecurity Practice



Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.



**Joanne Dynak**