Every Move You Make, I'll Be Watching You Watching Me Watching You

By Tanya Forsheit and Daniel Goldberg

Smart TVs, like other Internet-connected devices, come with their fair share of privacy and data security risks. This article explores a few noteworthy recent and high-profile developments that cast some doubt on the security of smart TVs and suggests that device manufacturers may not be sharing complete information about the data collected and used by those devices.

When we were kids, the notion of a smart TV with which we could interact was an unimaginable dream. You can't talk to a TV; that's crazy! But how cool would that be? SO cool. Today that fantasy is realty. Smart TVs are widely available and relatively inexpensive. In November 2015, Gartner forecasted that there will be more than 20 billion appliances, TVs, and other devices connected to the Internet by 2020.[1] Not surprisingly, smart TVs, like other Internet-connected devices, come with their fair share of privacy and data security risks.

This article explores a few noteworthy recent and high-profile developments, including news stories and regulatory enforcement, that cast some doubt on the security of smart TVs and suggests that device manufacturers may not be sharing complete information about the data collected and used by those devices. The article will also provide some key takeaways for how information security and privacy professionals can take a proactive role in helping their organizations that are building and marketing smart devices, including smart TVs, to build better safeguards, transparency, and consumer choices into these and all things that make up the "Internet of Things."

Privacy concerns

What exactly are "Smart TVs"? The United States Judicial Panel on Multidistrict Litigation defined them in one recent case as "televisions that have integrated Internet capability that supports direct streaming of movies and other programs from content providers such as Netflix, Hulu, and Amazon."[2]

Smart TVs necessarily raise issues related to their enhanced capacity for the collection, use, and sharing of sensitive consumer information. There are few laws that directly regulate such data processing. One notable exception is California's Business and Professions Code sections 22948.20-22948.25, which took effect January 1, 2016. It is one of a kind but limited in its application. The California law prohibits the operation of a voice recognition feature in an Internet-connected television without first prominently informing the user of the feature. It also prohibits the use or sale for advertising purposes of recordings of spoken words and conversations captured by a connected television for improving its voice recognition feature.

Although legislation is not there yet, the Federal Trade Commission's (FTC) recent settlement with smart TV manufacturer Vizio, Inc. (Vizio),[3] opens up a more in-depth discussion of the many privacy issues raised by smart TVs going beyond voice recognition data. As part of its recent focus on the Internet of Things (IoT) and smart devices, on February 6, 2017, the FTC in conjunction with the Office of the New Jersey Attorney General announced a settlement with Vizio, including payment of $1.5 million to the FTC and $1 million to the New Jersey Division of Consumer Affairs, with $300,000 of that

1 Nathan Eddy, "Gartner: 21 Billion IoT Devices to Invade By 2020," *InformationWeek*, November 10, 2015, available at http://www.informationweek.com/mobile/mobile-devices/gartner-21-billion-iot-devices-to-invade-by-2020/d/d-id/1323081.

2 *In re: Vizio, Inc., Consumer Privacy Litig.*, 176 F. Supp. 3d 1374, 1376 (U.S. Jud. Pan. Mult. Lit. 2016).

3 "VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent," FTC press release, available at https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it.

amount suspended, over claims that Vizio's smart TVs collected information about consumers' video-viewing behavior and shared that data with third parties without sufficient notice or consent.

The FTC's allegations (and pending class action litigation against Vizio involving similar issues) revolved around the "Smart Interactivity" feature found on Vizio's smart TVs. According to the FTC, starting in 2014, Vizio pre-installed its Smart Interactivity feature on new smart TVs and automatically installed the feature on older models. According to the complaint, only older models of the devices included a pop-up making consumers aware that the feature had been installed. The FTC alleged that Vizio described the feature as enabling "program offers and suggestions," which could be turned off through the smart TV settings.

The FTC's complaint went on to allege that the Smart Interactivity feature did not actually enable program offers or suggestions, but rather collected "highly-specific, second-by-second information" about consumers' video-viewing behaviors, including what content they watched, when they watched it, and the length of their views. Vizio allegedly determined what consumers watched by matching pixels from consumers' television screens with publicly available pixels from movies, shows, and commercials. Vizio then allegedly shared this viewing data, along with persistent identifiers it collected from consumers, with third-party data brokers in order to license that data to still other third parties for purposes of measuring audience viewership, determining advertising effectiveness, and serving targeted advertisements to specific consumers on their various devices. In its contracts with the data brokers, Vizio allegedly prohibited the data brokers from re-identifying consumers by name but allowed the data brokers to append data from their own internal databases such as sex, age, and income (thereby building a more robust consumer profile).

The FTC claimed that Vizio's actions violated Section 5 of the FTC Act[4] in three ways. First, the FTC alleged that Vizio acted unfairly by collecting and sharing sensitive information (i.e., video viewership information) without consumers' consent and through a medium consumers would not expect to be used for tracking. Second, the FTC alleged that Vizio deceived consumers by failing to adequately disclose that the Smart Interactivity feature collected and shared consumers' video viewership information. Finally, the FTC maintained that Vizio deceived consumers by falsely representing that the Smart Interactivity feature enabled program offers and suggestions when it actually collected and shared consumers' video viewership information.

Vizio's smart TVs collected information about consumers' video viewing behavior and shared that data with third parties without sufficient notice or consent.

It is worth noting the nature and status of the similar class action litigation as well. The television owners have contended that Vizio violates both the federal Video Privacy Protection Act ("VPPA")[5] and Wiretap Act[6] by tracking what consumers watch and selling that information to third-party data brokers and advertisers, exposing their personally identifiable information. In March 2017, a federal judge allowed the claims for violation of the VPPA, invasion of privacy, and intrusion upon seclusion to survive a motion to dismiss and granted plaintiffs leave to amend their allegations as to the Wiretap Act. The judge also allowed claims for fraudulent omission to move forward based on allegations that Vizio fraudulently hid its data practices by failing to mention the software it uses to collect data and how to disable the software or that the data is sold, despite a "very small font" privacy policy that claims the company collects anonymous and non-personal data.[7]

Privacy takeaways

What are the privacy takeaways for developers of smart TVs and other connected devices that are part of the Internet of Things?

- **Make accurate disclosures and do not omit material facts.** The FTC's primary concern with respect to Vizio appears to be that the company allegedly collected and

4 15 U.S.C. § 45, available at https://www.law.cornell.edu/uscode/text/15/45.

5 18 U.S. Code § 2710, available at https://www.law.cornell.edu/uscode/text/18/2710.

6 18 U.S. Code § 2511, available at https://www.law.cornell.edu/uscode/text/18/2511.

7 *In Re: Vizio, Inc., Consumer Privacy Litigation*, CASE NO. 8:16-ml-02693-JLS-KES (C.D. Cal. March 2, 2017).

shared video viewership information without accurately and fully disclosing its practices. Two of the three counts against Vizio involved deceptive acts or practices. According to the FTC, the alleged description of the Smart Interactivity feature was misleading and the pop-up, without further information, insufficient. Companies should carefully review the representations they make, including those made outside of their privacy policies.

- **Make sure your practices align with consumer expectations.** The FTC also voiced concern that Vizio's alleged practices of collecting and sharing video viewership information did not align with consumer expectations. Per the FTC, when using a television, consumers do not expect the television manufacturer to figure out exactly what they are watching and share that data with third parties for retargeting purposes. Manufacturers should understand that, even if a practice does not violate a specific statute, it may carry a "creepiness factor" that could attract regulatory scrutiny or impact a company's public perception and bottom line. To the extent companies intend to engage in such practices, companies should clearly and prominently alert consumers of their practices.
- **Get opt-in consent prior to sharing video viewership information**. In the Vizio settlement, the FTC refers to video viewership information as sensitive information that requires opt-in consent and potentially a separate video policy, prior to collection and sharing. Interestingly, acting Chairman Maureen Ohlhausen issued a concurring statement to the settlement questioning whether video viewership information should be treated as sensitive information. While there may be some disagreement over the sensitivity of video viewership information, legislators have taken the position that such data warrants greater scrutiny than many other forms of data (as evidenced by the federal VPPA and similar state laws). Under the VPPA, companies are prohibited from knowingly disclosing "personally identifiable information" concerning a consumer to any person unless an exception applies. There is currently a circuit split as to what constitutes personally identifiable information under the VPPA with some courts finding that video viewership information in conjunction with a static identifier (e.g., an IP address) is sufficient to plead a case. The VPPA and similar state laws provide consumers with a private right of action with an accompanying right to statutory damages even in the absence of a showing of harm.
- **Be creative with respect to your disclosures.** As part of settlement, the FTC required Vizio to prominently disclose its practices. The FTC emphasized that Vizio must provide unavoidable visual disclosures, and, more relevant for the IoT space, audible disclosures delivered in "a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand." Companies should view the audible disclosure requirement as a signal that the FTC expects IoT devices to provide conspicuous disclosures in a manner that is more aggressive than traditional small-print privacy policies linked to the bottom of web pages.
- **The $2.2 million payment does not tell the whole story.** Vizio allegedly collected video viewership information from more than 10 million televisions prior to entering into the settlement. So companies might think that the risk of a $2.2 million settlement seems minuscule in comparison to the potential upside. However, the settlement also requires Vizio to destroy all video viewing information collected without opt-in consent prior to March 1, 2016, establish a mandatory privacy program, have an independent third party routinely assess its data practices, keep extensive records and report to the FTC, and create new policies among other things. Thus, the real cost is significantly higher than $2.2 million.
- **Dealing with data brokers attracts scrutiny.** The FTC has shown consistent interest in regulating data brokers. For example, the FTC issued the report "Data Brokers: A Call for Transparency and Accountability" in May 2014 and the report "Big Data: A Tool for Inclusion or Exclusion" in January 2016. In the settlement with Vizio, the FTC specifically cited Vizio's contract prohibiting data brokers from re-identifying consumers yet allowing them to append certain forms of data. Smart device manufacturers should therefore be extra careful with regard to their practices when dealing with data brokers.

Data security issues

The hackability of connected devices, and smart TVs in particular, has been the subject of discussion for several years. There is something very intimate about the relationship between consumers and their televisions that makes this security vulnerability particularly compelling to the media and consumer advocates. And yet, it does not appear that much has changed with respect to the security (or lack thereof) in smart TVs since their emergence several years ago.

In December 2012, *Ars Technica* published a piece entitled "How an Internet-connected Samsung TV can spill your deepest secrets."[8] The story discussed the findings of a researcher who claimed at the time he had uncovered a vulnerability in most Samsung models that made it easy for him to locate their IP address on the Internet. Armed with this information, he claimed he could remotely access the device and exercise the same control someone in the same room would have, including gaining root access and installing malicious software.

> "At this point the attacker has complete control over the device," he wrote in an email to *Ars Technica*. "So we are talking about applying custom firmwares, spying on the victim if camera and microphone are available, stealing any credential and account stored...on the device, using his own certificates when accessing HTTPS websites, and

8 Dan Goodin, "How an Internet-Connected Samsung TV Can Spill Your Deepest Secrets," *Ars Technica*, 12/12/2012 https://arstechnica.com/security/2012/12/how-an-internet-connected-samsung-tv-can-spill-your-deepest-secrets/.

> tracking any activity of the victim (movies, photos, music, and websites seen) and so on. You become the TV."[9]

More than four years later, Wikileaks released a cache of documents in March 2017 purporting to show that the Central Intelligence Agency (CIA) hacked into smart TVs (and other smart devices) and that "[d]evelopers used vulnerabilities in Samsung TVs to ensure the products would capture conversations even when they appeared to be switched off…The CIA's engineering development group had a 'to do' list for the smart TV that included the ability to record video and break into its browser and apps."[10] There are even reports of smart TVs being hijacked by ransomware.[11]

Attacks on connected devices have consequences for the larger Internet as a whole. In October 2016, it was discovered that a major distributed denial of service (DDoS) attack was caused by a botnet largely made up of connected IoT devices.[12]

The law is not well equipped to incentivize device manufacturers to build in more robust security controls or design with privacy in mind. Existing state and federal data breach notification laws generally cover only certain narrow categories of information such as name with Social Security number, driver's license number, payment card information, health or medical information, but a few state laws have been expanded to require notification when usernames and/or email addresses together with passwords and/or security questions and answers are exfiltrated. However, a security breach involving a smart TV is more likely to involve information about a user's viewing habits or movements as opposed to these more traditional categories of personally identifying information.

It seems somewhat more likely that continued enforcement from the FTC and European regulators, and private class action litigation, will serve as an instigator. The $2.2 million fine, order to delete previously collected data, and years of oversight imposed on Vizio is not nothing, not to mention what must be extraordinary legal fees to negotiate with the FTC and defend dozens of class actions that are now before the United States Judicial Panel on Multidistrict Litigation in the Central District of California. Further, when the EU General Data Protection Regulation takes effect in May 2018, even US companies that process personal data (broadly defined to include device identifiers for smart TVs and similar devices) of EU data subjects will be forced to comply with more significant privacy and data security obligations or face penalties of up to four percent of global turnover or €20 million.

But we all know that the law is ultimately incapable of keeping up with technology, which will continue to advance at breakneck speed. Industry self-regulatory efforts in the smart device world are likely to be a much more effective and practical solution to meet the concerns of regulators and consumers alike and to take steps, if only modest, to beat back bad actors who would seek to hack into the majority of American living rooms and bedrooms. There is already such industry action in a number of IoT sectors, including connected cars. In 2014, the Alliance of Automobile Manufacturers and the Association of Global Automakers proposed a set of privacy principles for vehicle technologies and services.[13] It does not appear that the Consumer Technology Association has yet taken similar steps vis-à-vis smart TVs or other connected home devices.

Information security professionals can play a critical role by bringing these issues to the attention of other relevant stakeholders within the organization, particularly those involved in design and marketing, legal, and compliance. Information security professionals are ideally situated to help develop products with better security in mind, right from the start. They should have a seat at the table during the product development stage.

Conclusion

Smart TVs and other connected home devices are here to stay. As with so many other technology verticals, it would behoove the consumer electronics industry, policy makers, and consumer advocates alike to work together to put forth a set of appropriate, risk-based, self-regulatory principles to help ensure that privacy interests are protected and information security advanced without stifling innovation.

About the Authors

Tanya Forsheit is co-chair of Frankurt Kurnit Klein + Selz's Privacy & Data Security Group, and a partner in the Technology & Digital Media, Litigation, and Advertising, Marketing & Public Relations groups. She represents multi-national and emerging companies in the media, entertainment, consumer products, health care, technology, and professional services industries, and serves as outside privacy counsel for numerous organizations. She may be reached at tforsheit@fkks.com.

Daniel M. Goldberg is an associate in Frankurt Kurnit Klein + Selz's Privacy & Data Security Group focusing on advertising, branded entertainment, interactive entertainment, technology, digital media and privacy, and intellectual property matters. He represents multi-national and emerging companies in a wide range of privacy and data security-related matters involving the collection, use, storage, and monetization of confidential data. He may be reached at dgoldberg@fkks.com.

9 Ibid.

10 Hannah Kuchler, "The Internet of Things: Home Is Where the Hackers Are," *Financial Times*, March 10, 2017, available at https://www.ft.com/content/cb880bc2-057c-11e7-ace0-1ce02ef0def9.

11 Ibid.

12 Nicky Woolf, "DDoS Attack That Disrupted Internet was Largest of Its Kind in History, Experts Say," *The Guardian*, October 26, 2016, available at https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

13 Jules Polonetsky, "Connected cars are accelerating consumer benefits and driving privacy issues," The Hill, November 21, 2014, available at http://thehill.com/blogs/pundits-blog/technology/224954-connected-cars-are-accelerating-consumer-benefits-and-driving.