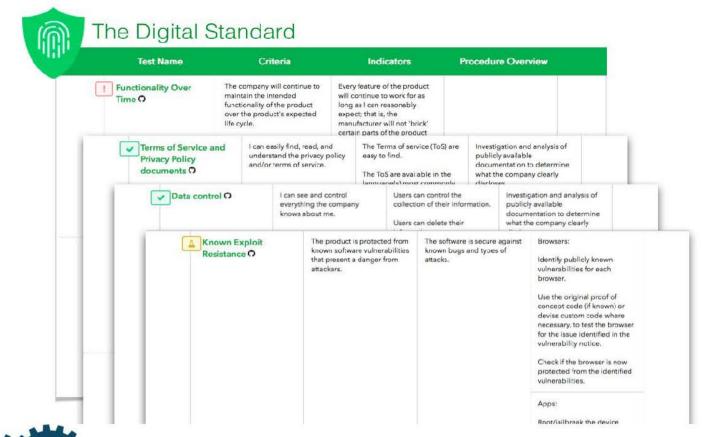
Evaluation of the Privacy and Security Aspects of Connected Televisions





Summary of TV findings

- Investigated 5 TVs:
 - LG, Samsung, Vizio, Sony, and TCL/Roku
- In partnership with Ranking Digital Rights and Disconnect
- Looked at policies, consent flows, data flows, security vulnerabilities



Summary of TV findings

- All models want to watch what you're watching
 - Via "automatic content recognition"
- Could limit data collection, but compromised functionality
- Security vulnerabilities in some of the TVs



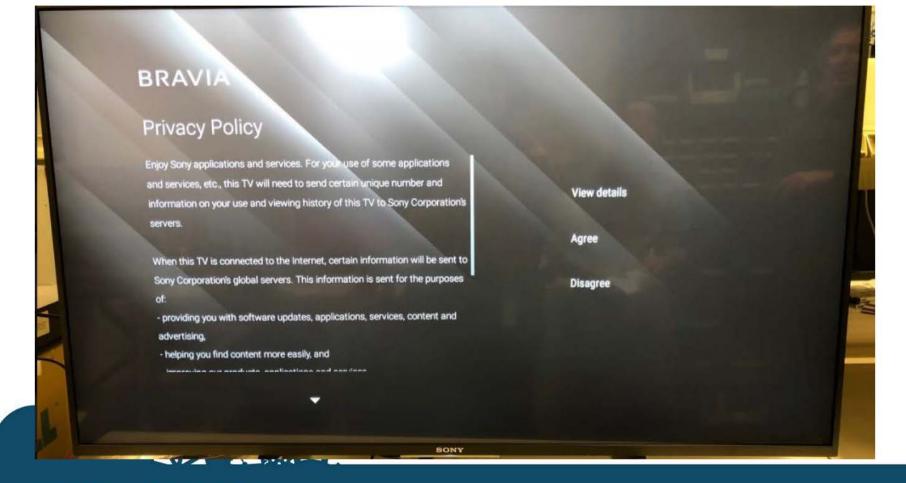
Context: Vizio settlement

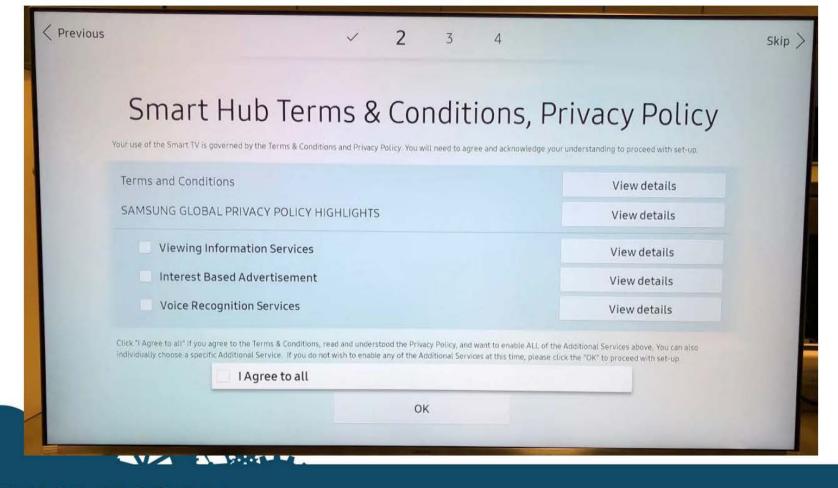
- FTC settled with Vizio for \$1.5 million in February 2017
- Collection of viewing activity without consent deemed an "unfair practice"
- Commr. Ohlhausen concurrence: Viewing is considered "sensitive" information under US law



What does consent look like?



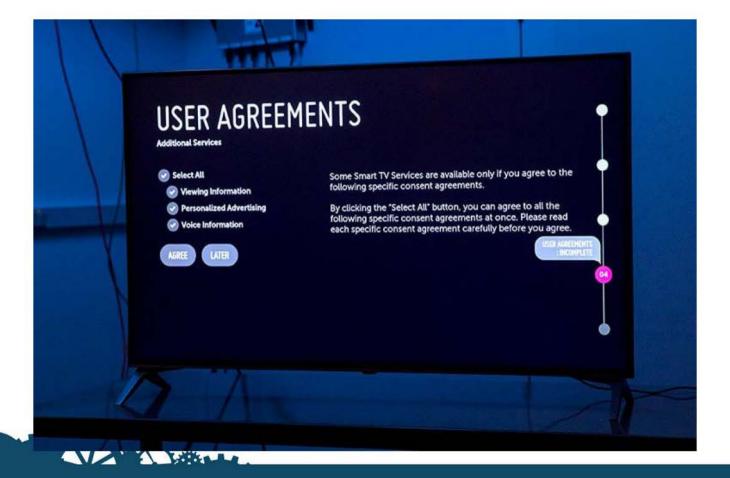




Loss of functionality

 You could always control collection of viewing data, but with a cost to functionality







Post set-up controls

- All of the televisions offered controls in Settings to limit data collection
 - All gave you the ability to stop collection of viewing data
 - BUT, controls were usually hard to find



Post set-up controls

- Vizio: Settings → System → Reset and Admin
- Roku: Settings → Privacy → Smart TV Experience



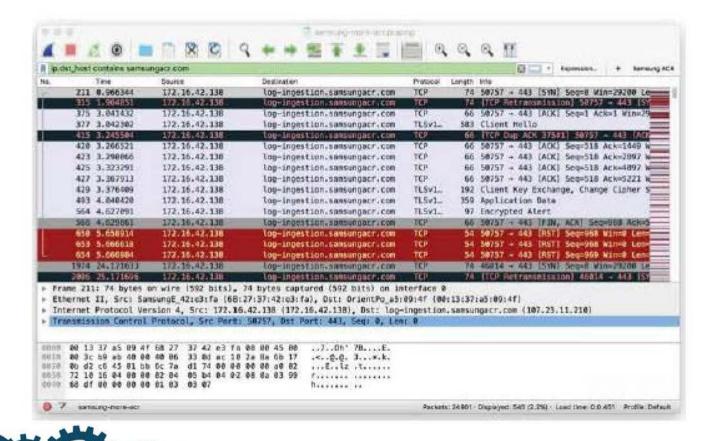
How much control?

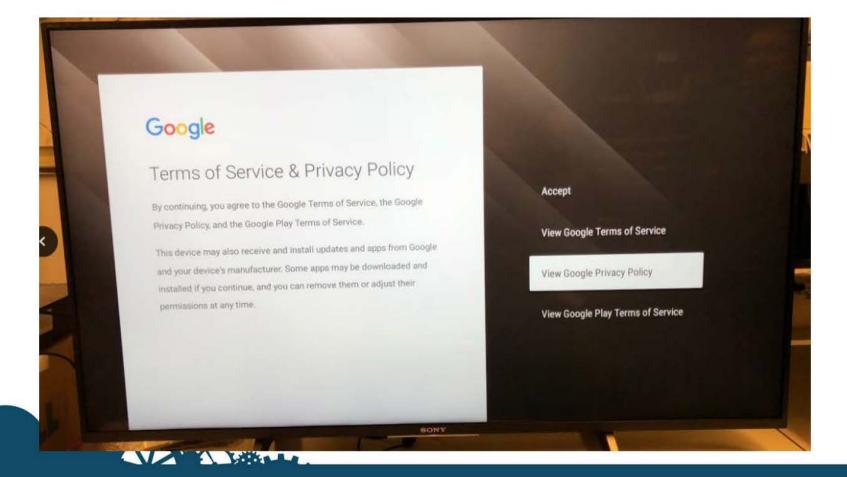
 Scope of controls and data collection was sometimes unclear

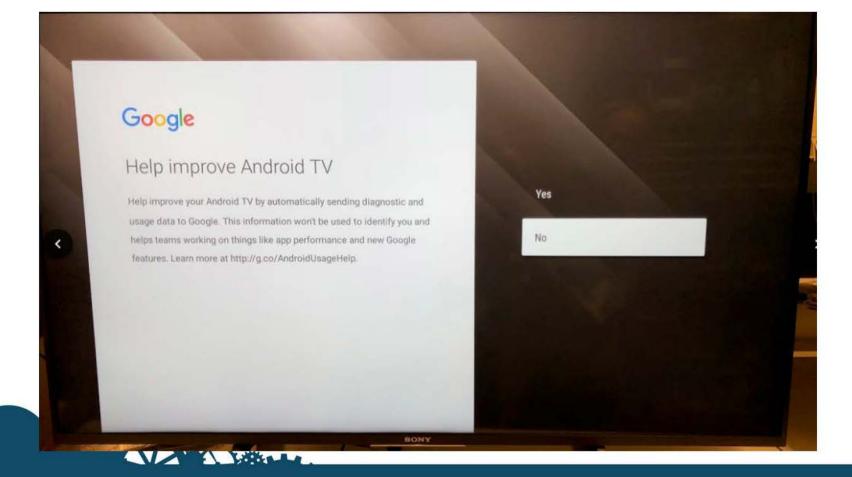


Please visit the "settings" menu of your Smart TV for choices that may be available to you if you do not wish to continue to receive personalized recommendations or certain enhanced features on your Smart TV. If you disable such personalized recommendations or additional features, then the information and content displayed on your Smart TV may not be as relevant to you. But please bear in mind that Samsung may still collect information about your usage of the Smart TV for other purposes as described in the main body of this Privacy Policy.









Security vulnerabilities

- Discovered vulnerabilities in the Roku OS and Samsung API's that allowed hackers to manipulate the television
 - Change channel or volume, disconnect from internet
 - No evidence that information was vulnerable, or that hackers could leverage holes to access other devices



Future work

- More detailed findings about Smart TVs
- Similar investigations into other products
- Incorporate into standard ratings process where appropriate
- Other criteria: interoperability, repairability

