Consumer Reports
Digital Standard Test Summary Notes

Examining data privacy & data security in
Smart Televisions | 2019 Models | June 2020

Purpose of this document:

This document is what our testing team uses to record a summary of our testing process and findings. It includes information about testing methodology, highlights, and overall suggestions for improvement of this product category. It helps the team describe any significant insights of our current test batch.

How-to read this document:

- Section 1: An overview of testing methodology.
- Section 2: Highlights of some good practices and specific problems or issues we found in certain companies' products and some common industry-wide problems or issues.
- Section 3: Overall suggestions for improvement in this product area, explaining what changes we are looking for manufacturers to make in the interest of consumers.

Who was this created for?

This document is intended to summarize the key test results to the content creators and other colleagues within Consumer Reports, who may then use this information to produce material targeted to various audiences or platforms, such as a Consumer Reports article tailored for more public consumption.

Section 1: Methodology

Smart TVs were already a part of CR's testing program. Because of the potential digital privacy and security concerns in connecting these televisions to the internet and sharing data with tech companies, we conducted an evaluation of Data Privacy and Data Security aspects of the smart TVs' functionality and manufacturers, focused on the following criteria from the Digital Standard (thedigitalstandard.org):

Data Privacy	Data Security
PP and ToS Documents	Best Build Practices
PP and ToS Update Notification	Authentication
Data Control	Encryption
Data Sharing	Known Exploit Resistance
Data Use	Security Oversight
Data Retention and Deletion	Security over time
Data benefits	Vulnerability Disclosure program
Data Collection	
Minimal data collection	
Privacy by default	
Privacy Setting EOU	

Our evaluation process has three parts.

- Inspection of TV Screens and Settings
    - We evaluate the TV setup process regarding privacy settings.
    - We check the account registration for personal information collection and the account authentication system.
    - We review the TV settings menu and look for post-setup controls related to data privacy and security.
    - We review the mobile app settings menu and look for post-setup controls related to data privacy and security.
    - We also look for other information to help us to understand how the software/firmware is designed and what services are implemented in TVs. (eg. kernel version, firmware version, voice assistance system, automatic content recognition, etc.)
- Light security audit
    - We run static analysis and dynamic analysis on the mobile remote application.
    - We capture and analyze network traffic on smart TVs.
    - We research common vulnerabilities and data exposures on smart TVs.

  - We conduct light penetration tests and disclose responsibly to companies if we find security vulnerabilities or bugs.
- Document Review
  - We gather privacy policies, terms of service, and other readily accessible public information for document review.
  - We evaluate claims and quotes from those documents to understand how companies may handle users' data.

Our testing includes evaluation of 50+ indicator statements, which are the attributes needed for a product to meet the specified Digital Standard criteria. The 5 most important indicators for Data Privacy and Data Security are as follows:

Top Indicators for Data Privacy

- The company puts limits on the use of users' data that is consistent with the purpose for which the data is collected.
- The company explicitly discloses every way in which it utilizes users' data
- The user information collected is only that which is directly relevant and necessary for the service
- Targeted advertising is off by default
- User interface settings that are optimal for privacy are set by default

Top Indicators for Data Security:

- The product was built with effectively implemented safety features
- Transmission of user communication is encrypted by default
- The software is secure against known bugs and types of attacks
- The product life cycle is communicated to the potential owner before purchase
- The software can be kept up-to-date for security issues.

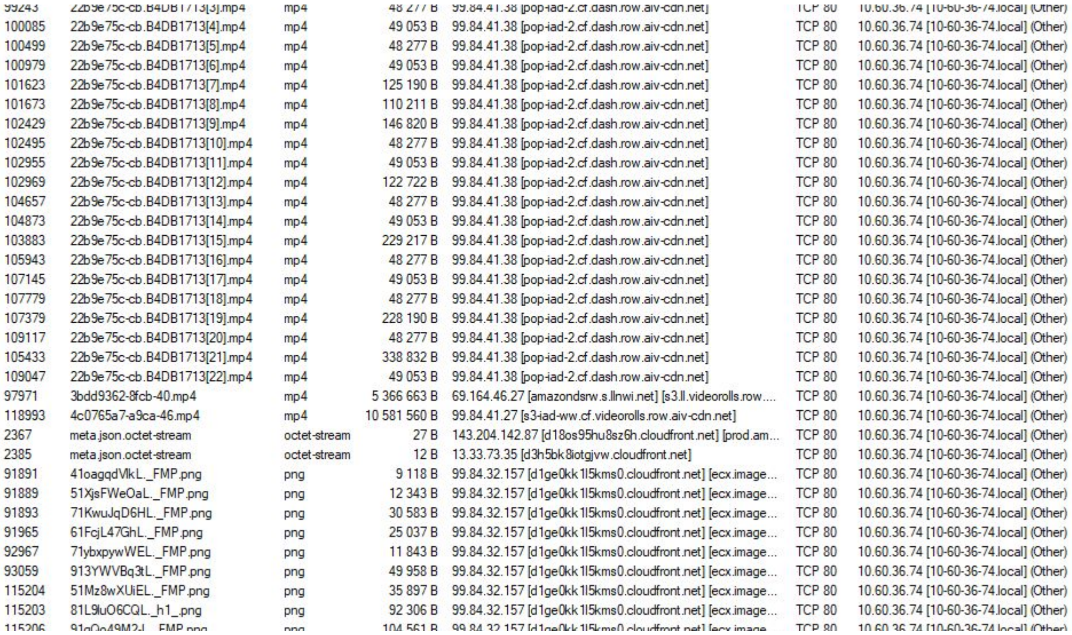
Section 2: Key Findings

Data Security

- Authentication
  - In contrast to other brands, Roku TVs did not implement authentication for their remote control APIs.
  - Examples of other sub-optimal practices:
    - No brand's app provided an option to let the user select requiring a login for every use.
    - FireTV, Roku, and Vizio had weak password creation rules (e.g., a password of 111111 was allowable,) although Vizio account registration was optional.
    - Roku required the user to register an account with them in order to use

        the TV.
        - Fire TV required the user to register and sign in to an Amazon account to use full features.

- Encryption
    - Roku encrypted all traffic in our test.
    - LG, Sony, and Vizio had a few cases of unencrypted network traffic. However, it did not appear that any meaningful information was leaked.
    - Samsung had many cases of unencrypted network traffic. However, it did not appear that any meaningful information was leaked.
    - Fire TV had many cases of unencrypted traffic, including pre-load video clips and images which we were able to watch from the network traffic capture file.

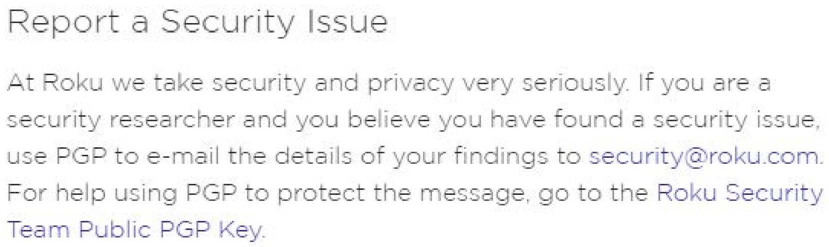


99243	22b9e75c-cb.B4DB1713[3].mp4	mp4	48 277 B	99.84.41.38 [pop-iad-2.cf.dash.row.aiv-cdn.net]	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
100085	22b9e75c-cb.B4DB1713[4].mp4	mp4	49 053 B	99.84.41.38 [pop-iad-2.cf.dash.row.aiv-cdn.net]	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
100499	22b9e75c-cb.B4DB1713[5].mp4	mp4	48 277 B	99.84.41.38 [pop-iad-2.cf.dash.row.aiv-cdn.net]	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
100979	22b9e75c-cb.B4DB1713[6].mp4	mp4	49 053 B	99.84.41.38 [pop-iad-2.cf.dash.row.aiv-cdn.net]	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
101623	22b9e75c-cb.B4DB1713[7].mp4	mp4	125 190 B	99.84.41.38 [pop-iad-2.cf.dash.row.aiv-cdn.net]	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
101673	22b9e75c-cb.B4DB1713[8].mp4	mp4	110 211 B	99.84.41.38 [pop-iad-2.cf.dash.row.aiv-cdn.net]	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
102429	22b9e75c-cb.B4DB1713[9].mp4	mp4	146 820 B	99.84.41.38 [pop-iad-2.cf.dash.row.aiv-cdn.net]	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
102495	22b9e75c-cb.B4DB1713[10].mp4	mp4	48 277 B	99.84.41.38 [pop-iad-2.cf.dash.row.aiv-cdn.net]	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
102955	22b9e75c-cb.B4DB1713[11].mp4	mp4	49 053 B	99.84.41.38 [pop-iad-2.cf.dash.row.aiv-cdn.net]	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
102969	22b9e75c-cb.B4DB1713[12].mp4	mp4	122 722 B	99.84.41.38 [pop-iad-2.cf.dash.row.aiv-cdn.net]	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
104657	22b9e75c-cb.B4DB1713[13].mp4	mp4	48 277 B	99.84.41.38 [pop-iad-2.cf.dash.row.aiv-cdn.net]	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
104873	22b9e75c-cb.B4DB1713[14].mp4	mp4	49 053 B	99.84.41.38 [pop-iad-2.cf.dash.row.aiv-cdn.net]	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
103883	22b9e75c-cb.B4DB1713[15].mp4	mp4	229 217 B	99.84.41.38 [pop-iad-2.cf.dash.row.aiv-cdn.net]	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
105943	22b9e75c-cb.B4DB1713[16].mp4	mp4	48 277 B	99.84.41.38 [pop-iad-2.cf.dash.row.aiv-cdn.net]	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
107145	22b9e75c-cb.B4DB1713[17].mp4	mp4	49 053 B	99.84.41.38 [pop-iad-2.cf.dash.row.aiv-cdn.net]	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
107779	22b9e75c-cb.B4DB1713[18].mp4	mp4	48 277 B	99.84.41.38 [pop-iad-2.cf.dash.row.aiv-cdn.net]	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
107379	22b9e75c-cb.B4DB1713[19].mp4	mp4	228 190 B	99.84.41.38 [pop-iad-2.cf.dash.row.aiv-cdn.net]	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
109117	22b9e75c-cb.B4DB1713[20].mp4	mp4	48 277 B	99.84.41.38 [pop-iad-2.cf.dash.row.aiv-cdn.net]	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
105433	22b9e75c-cb.B4DB1713[21].mp4	mp4	338 832 B	99.84.41.38 [pop-iad-2.cf.dash.row.aiv-cdn.net]	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
109047	22b9e75c-cb.B4DB1713[22].mp4	mp4	49 053 B	99.84.41.38 [pop-iad-2.cf.dash.row.aiv-cdn.net]	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
97971	3bdd9362-8fcb-40.mp4	mp4	5 366 663 B	69.164.46.27 [amazondsrw.s.llnwi.net] [s3.ll.videorolls.row....	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
118993	4c0765a7-a9ca-46.mp4	mp4	10 581 560 B	99.84.41.27 [s3-iad-ww.cf.videorolls.row.aiv-cdn.net]	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
2367	meta.json.octet-stream	octet-stream	27 B	143.204.142.87 [d18os95hu8sz6h.cloudfront.net] [prod.am...	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
2385	meta.json.octet-stream	octet-stream	12 B	13.33.73.35 [d3h5bk8iotgjvw.cloudfront.net]	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
91891	41oagqdVlkL._FMP.png	png	9 118 B	99.84.32.157 [d1ge0kk1l5kms0.cloudfront.net] [ecx.image...	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
91889	51XjsFWeOaL._FMP.png	png	12 343 B	99.84.32.157 [d1ge0kk1l5kms0.cloudfront.net] [ecx.image...	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
91893	71KwuJqD6HL._FMP.png	png	30 583 B	99.84.32.157 [d1ge0kk1l5kms0.cloudfront.net] [ecx.image...	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
91965	61FcjL47GhL._FMP.png	png	25 037 B	99.84.32.157 [d1ge0kk1l5kms0.cloudfront.net] [ecx.image...	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
92967	71ybxpywWEL._FMP.png	png	11 843 B	99.84.32.157 [d1ge0kk1l5kms0.cloudfront.net] [ecx.image...	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
93059	913YWVBq3tL._FMP.png	png	49 958 B	99.84.32.157 [d1ge0kk1l5kms0.cloudfront.net] [ecx.image...	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
115204	51Mz8wXUiEL._FMP.png	png	35 897 B	99.84.32.157 [d1ge0kk1l5kms0.cloudfront.net] [ecx.image...	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
115203	81L9luO6CQL._h1_.png	png	92 306 B	99.84.32.157 [d1ge0kk1l5kms0.cloudfront.net] [ecx.image...	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)
115206	91qOo49M2-L._FMP.png	png	104 561 B	99.84.32.157 [d1ge0kk1l5kms0.cloudfront.net] [ecx.image...	TCP 80	10.60.36.74 [10-60-36-74.local] (Other)

MP4 Files were not encrypted on a FireTV

- Security Over Time
    - Example of good practices: All TVs provided either an automatic update or push update notification which the user could update by “one-click”.
    - However, no company disclosed the length of time they would support the software for their product.

- Vulnerability Disclosure Program
    - Roku did not describe the details of a vulnerability disclosure program. They only provided a contact email.
    - Vizio did not describe the details of a vulnerability disclosure program. However, some descriptions from Google would apply because Vizio TVs were based on Google Chrome.



Report a Security Issue

At Roku we take security and privacy very seriously. If you are a security researcher and you believe you have found a security issue, use PGP to e-mail the details of your findings to security@roku.com. For help using PGP to protect the message, go to the Roku Security Team Public PGP Key.

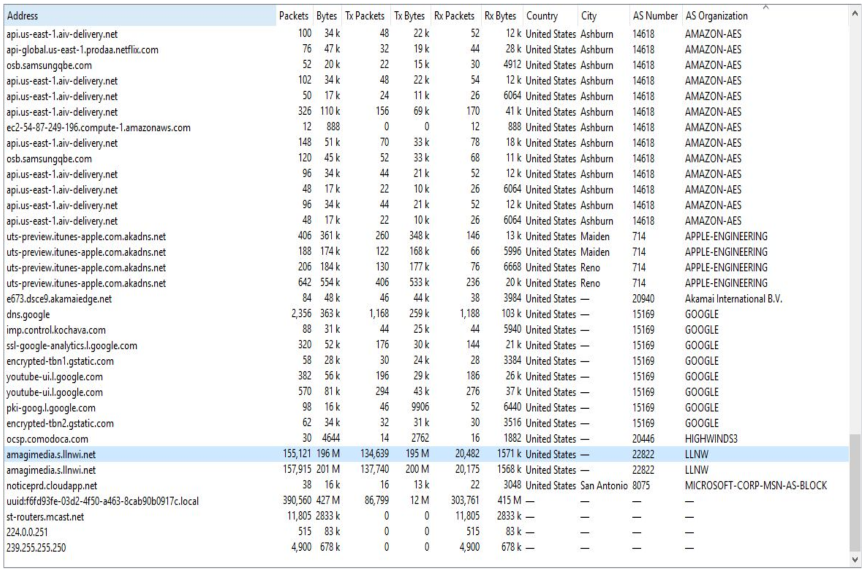
Roku’s vulnerability reporting message

Data Privacy

As part of the Data Privacy assessment, we gathered privacy policies, terms of service, and other readily accessible public information for document review, and we evaluated claims and quotes from those documents to understand how companies said they handle users’ data. The following points from this documentation indicate some sub-optimal (from a consumer perspective) practices or lack of transparency

Samsung

1. Data Control - The company indicated that disabling data collection could prevent the use of some features of the device or service.
2. Data Control - The company provided the user with the option to opt-out of some data collection, but it is unclear whether or not this will stop additional data collection used for targeted ads.
3. Data Collection - The company stated that user information is collected from third parties, but did not provide significant detail about the types of data collected from third parties.
4. Data Sharing - According to our network traffic record, Samsung smart TVs communicated with a geo-targeted advertising company called Amagimedia. However, we did not find Amagimedia mentioned in its privacy policy.



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
api.us-east-1.aiv-delivery.net	100	34 k	48	22 k	52	12 k	United States	Ashburn	14618	AMAZON-AES
api-global.us-east-1.prodaa.netflix.com	76	47 k	32	19 k	44	28 k	United States	Ashburn	14618	AMAZON-AES
osb.samsungqbe.com	52	20 k	22	15 k	30	4912	United States	Ashburn	14618	AMAZON-AES
api.us-east-1.aiv-delivery.net	102	34 k	48	22 k	54	12 k	United States	Ashburn	14618	AMAZON-AES
api.us-east-1.aiv-delivery.net	50	17 k	24	11 k	26	6064	United States	Ashburn	14618	AMAZON-AES
api.us-east-1.aiv-delivery.net	326	110 k	156	69 k	170	41 k	United States	Ashburn	14618	AMAZON-AES
ec2-54-87-249-196.compute-1.amazonaws.com	12	888	0	0	12	888	United States	Ashburn	14618	AMAZON-AES
api.us-east-1.aiv-delivery.net	148	51 k	70	33 k	78	18 k	United States	Ashburn	14618	AMAZON-AES
osb.samsungqbe.com	120	45 k	52	33 k	68	11 k	United States	Ashburn	14618	AMAZON-AES
api.us-east-1.aiv-delivery.net	96	34 k	44	21 k	52	12 k	United States	Ashburn	14618	AMAZON-AES
api.us-east-1.aiv-delivery.net	48	17 k	22	10 k	26	6064	United States	Ashburn	14618	AMAZON-AES
api.us-east-1.aiv-delivery.net	96	34 k	44	21 k	52	12 k	United States	Ashburn	14618	AMAZON-AES
api.us-east-1.aiv-delivery.net	48	17 k	22	10 k	26	6064	United States	Ashburn	14618	AMAZON-AES
uts-preview.itunes-apple.com.akadns.net	406	361 k	260	348 k	146	13 k	United States	Maiden	714	APPLE-ENGINEERING
uts-preview.itunes-apple.com.akadns.net	188	174 k	122	168 k	66	5996	United States	Maiden	714	APPLE-ENGINEERING
uts-preview.itunes-apple.com.akadns.net	206	184 k	130	177 k	76	6668	United States	Reno	714	APPLE-ENGINEERING
uts-preview.itunes-apple.com.akadns.net	642	554 k	406	533 k	236	20 k	United States	Reno	714	APPLE-ENGINEERING
e673.dsce9.akamaiedge.net	84	48 k	46	44 k	38	3984	United States	—	20940	Akamai International B.V.
dns.google	2,356	363 k	1,168	259 k	1,188	103 k	United States	—	15169	GOOGLE
imp.control.kochava.com	88	31 k	44	25 k	44	5940	United States	—	15169	GOOGLE
ssl-google-analytics.l.google.com	320	52 k	176	30 k	144	21 k	United States	—	15169	GOOGLE
encrypted-tbn1.gstatic.com	58	28 k	30	24 k	28	3384	United States	—	15169	GOOGLE
youtube-ui.l.google.com	382	56 k	196	29 k	186	26 k	United States	—	15169	GOOGLE
youtube-ui.l.google.com	570	81 k	294	43 k	276	37 k	United States	—	15169	GOOGLE
pki-goog.l.google.com	98	16 k	46	9906	52	6440	United States	—	15169	GOOGLE
encrypted-tbn2.gstatic.com	62	34 k	32	31 k	30	3516	United States	—	15169	GOOGLE
ocsp.comodoca.com	30	4644	14	2762	16	1882	United States	—	20446	HIGHWINDS3
amagimedia.s.llnwi.net	155,121	196 M	134,639	195 M	20,482	1571 k	United States	—	22822	LLNW
amagimedia.s.llnwi.net	157,915	201 M	137,740	200 M	20,175	1568 k	United States	—	22822	LLNW
noticeprd.cloudapp.net	38	16 k	16	13 k	22	3048	United States	San Antonio	8075	MICROSOFT-CORP-MSN-AS-BLOCK
uuid:f6fd93fe-03d2-4f50-a463-8cab90b0917c.local	390,560	427 M	86,799	12 M	303,761	415 M	—	—	—	—
st-routers.mcast.net	11,805	2833 k	0	0	11,805	2833 k	—	—	—	—
224.0.0.251	515	83 k	0	0	515	83 k	—	—	—	—
239.255.255.250	4,900	678 k	0	0	4,900	678 k	—	—	—	—

Network Traffic From a Samsung Smart TV

Roku

1. Data Control - The company stated that only those who are affected by CCPA regulations may obtain a copy of their personal information.
2. Data Control - A portability service was stated to be available only to those who are affected by CCPA regulations.
3. Data Sharing - The company provided little information or reference to only sharing what is necessary for the service. There is a statement that said that they may share personal information with affiliates for their own reasons. The reasons are undefined. The company claimed that they sell or "may freely share" aggregated or anonymized data derived from personal data.
4. Data Collection - The company stated that user information is acquired from third parties, but does not provide meaningful detail about the types of data collected.

Samba TV (Sony Smart TV)

1. Data Sharing - The company provided little information or reference to only sharing what is necessary for the service. There was a statement that they may share personal information with affiliates for their own reasons. The reasons are undefined. The company claims that they sell or "may freely share" aggregated or anonymized data derived from personal data.
2. Data benefits - The company made some references as to why certain pieces of data are collected, however, references were scant or vague. It did include information collection justifications in regard to the device or service under test (ACR).

LG

1. Data Use - The company stated they use data only for necessary services. However, their documentation was not clear about what they consider to be necessary.
2. Data Retention and Deletion - The company stated that user data is an asset that will be transferred.
3. Data Collection - The company clearly stated that they collect user information from third parties, but did not provide additional information about the precise types of information collected from third parties.

Section 3: Overall Suggestions for Companies

Data Security

- Most companies did well in implementing encryption to protect user's sensitive data and had implemented protections against previously known exploits.
- However, there are some common issues found by our Security evaluation that are areas for improvement:
    - Security Oversight
        - Companies should disclose if they have policies and processes to limit employees' access to users' data. (Like ACR data)
        - Companies should disclose the security audit measures they have put in place for their product or server.
    - Security over time
        - Most consumers expect their TVs to last for a number of years. Unsupported smart TVs could be vulnerable to new exploits if they are no longer receiving security updates. Companies should clearly disclose the support period for their products so that consumers can know what the support period is before they decide to purchase that product.
    - Vulnerability Disclosure program
        - Companies should set up proper vulnerability disclosure programs for security researchers to report the vulnerabilities or bugs they found. Good practices for this would include::
            - Having an easy access portal from the official website or a well-known bug bounty site (like HackerOne)
            - Disclosing the estimated timeline of the process
            - Committing to not pursue legal action on security researchers who report bugs or vulnerabilities.

Data Privacy

- Our privacy evaluation consisted of reviewing device controls and UI settings, as well as reviewing the publicly available documentation. Overall, there are many areas where companies can improve their Data Privacy practices or transparency:

- Data Control
  - Provide features and instructions for users to turn on/off data collection, obtain a copy of the data collected about them, and delete the data collected about them. This control should include ACR, targeted advertising, usage data, and other personal data.
  - Practices that were put in place to satisfy California or European privacy standards should be available to all consumers, even if they're not in California or the EU.
- Data Sharing
  - Make it clear what data is shared and with whom, or if data is not rented or shared data with anyone.
- Data Use
  - Commit to using consumers' data only to provide services to the user
  - Disclose how user data (such as ACR data) is used.
- Data Retention and Deletion
  - Disclose how long user data is retained.
  - Commit to delete the data after users delete their account
- Privacy by default
  - All settings in the user interface should be optimal for privacy by default.