FEDERAL TRADE COMMISSION
Washington, DC 20580

In the Matter of	)
	)
Samsung Electronics Co., Ltd.	)
	)
	)

Complaint, Request for Investigation, Injunction, and Other Relief

Submitted by

The Electronic Privacy Information Center

I. Introduction

1. This complaint concerns certain business practices of Samsung Electronics, Ltd. that adversely impact consumer privacy in the United States. As set forth in detail below, Samsung routinely intercepts and records the private communications of consumers in their homes. Consumers who have learned of this practices have described it is as both "unfair" and "deceptive." Samsung's attempts to disclaim its intrusive surveillance activities by means of a "privacy notice" do not diminish the harm to American consumers. It is incumbent upon the Federal Trade Commission to take action in this matter, and to enjoin Samsung and other companies that engage in similar practices, from such unlawful activities.

II. Parties

2. The Electronic Privacy Information Center ("EPIC") is a public interest research center located in Washington, D.C. EPIC focuses on emerging privacy and civil liberties issues and is a leading consumer advocate before the FTC. EPIC has a particular interest in protecting consumer privacy, and has played a leading role in developing the authority of the FTC to address emerging privacy issues and to safeguard the privacy rights of consumers.[1] In 2013 EPIC filed an FTC complaint against Samsung's mobile app for Jay-Z's new album "Magna Carta Holy Grail"

[1] *See, e.g.*, Letter from EPIC Exec. Dir. Marc Rotenberg to FTC Comm'r Christine Varney (Dec. 14, 1995) (urging the FTC to investigate the misuse of personal information by the direct marketing industry), http://epic.org/privacy/internet/ftc/ftc_letter.html; DoubleClick, Inc., *FTC* File No. 071-0170 (2000) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf; Microsoft Corporation, FTC File No. 012 3240 (2002) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/consumer/MS_complaint.pdf; Choicepoint, Inc., FTC File No. 052-3069 (2004) (Request for Investigation and for Other Relief) , http://epic.org/privacy/choicepoint/fcraltr12.16.04.html.

for using unnecessarily invasive software that "deprived users of meaningful choice regarding the collection of their data."[2] EPIC's complaint concerning Google Buzz provided the basis for the Commission's investigation and subsequent settlement concerning the social networking service.[3] The Commission's settlement with Facebook also followed from a Complaint filed by EPIC and a coalition of consumer privacy organizations.[4] EPIC has previously urged the Commission to investigate businesses that make misleading representations as to record destruction practices. EPIC's complaint against several purveyors of stalker spyware led to a permanent injunction banning the further distribution of the malicious computer software.[5] Following EPIC's complaint, the FTC successfully petitioned a federal court for a permanent injunction barring sales of CyberSpy's "stalker spyware," over-the-counter surveillance technology allowing individuals to spy on other individuals.[6] EPIC also previously notified the Commission that AskEraser falsely represented that search queries would be deleted when in fact they were retained by the company and made available to law enforcement agencies.[7]

3. Samsung Electronics Co., Ltd., is a Republic of Korea limited company with its principal place of business in 250, 2-gaaepyong-ro, Jung-gu, Seoul 100-742, Korea. Samsung Electronics America, Inc. is a subsidiary of Samsung Electronics Co., Ltd., located at 105 Challenger Road Ridgefield Park, N.J. 07660.[8] Dozens of affiliates and subsidiaries operate under the Samsung brand, including Samsung Electronics, one of the largest electronics manufacturers in the world. One of Samsung Electronics' most successful enterprises has been its manufacture of

---

[2] In re Samsung, (2013) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/ftc/EPICsamsungcomplaintFINAL.pdf. *See also,* EPIC: Samsung 'Jay-Z Magna Carta' App, https://epic.org/samsung_jay-z_magna_carta_app.html (last visited Feb. 11,

[3] Press Release, Federal Trade Comm'n, FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network (Mar. 30, 2011), http://ftc.gov/opa/2011/03/google.shtm ("Google's data practices in connection with its launch of Google Buzz were the subject of a complaint filed with the FTC by the Electronic Privacy Information Center shortly after the service was launched."). The Commission found that Google "used deceptive tactics and violated its own privacy promises to consumers when it launched [Buzz]."

[4] In the Matter of Facebook, Inc., (2009) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf [hereinafter EPIC 2009 Facebook Complaint]; In the Matter of Facebook, Inc., (2010) (EPIC Supplemental Materials in Support of Pending Complaint and Request for Injunction, Request for Investigation and for Other Relief), https://*epic.org/privacy/inrefacebook/EPIC_Facebook_Supp.pdf* [hereinafter EPIC 2009 Facebook Supplement]; In the Matter of Facebook, Inc., (2010) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief) , https://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf [hereinafter EPIC 2010 Facebook Complaint].

[5] In the Matter of Awarenesstech.com, et al., (2008) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/dv/spy_software.pdf.

[6] FTC v. CyberSpy Software, LLC, No. 6:08-cv-1872-Orl-31GJK, 2009 WL 2386137 (M.D. Fla. July 31, 2009) (Order), *available at*
http://www.ftc.gov/sites/default/files/documents/cases/2010/06/100602cyberspystip.pdf.

[7] EPIC: Does AskEraser Really Erase?, https://epic.org/privacy/ask/

[8] *Contact Us*, SAMSUNG, http://www.samsung.com/us/business/contact_us.html (last visited Feb. 10, 2015).

"Smart TVs" – home entertainment systems that respond to human voices and gestures.[9]

II. Factual Background

A. Congress Anticipated the Privacy Threats of "Interactive Television" In the Early 1980s.

4. Concerns about the use of televisions to collect consumer information were anticipated in the 1980s.[10]

5. Privacy concerns grew out of an awareness that televisions would enable a wide range of functions in the home, including "home banking, instant voting, storage of personal information, home shopping, instant-response study courses, automatic regulation of utility use, a selection from almost 1,000 data bases of specialized information, and security services which can monitor for fire, home intrusion and medical emergency."[11]

6. The initial deployment of occurred through the "set-top" boxes that delivered cable television to the consumer, and transmited user data to the service provider.[12]

7. Privacy scholars and policy makers recognized the risk that interactive television would threaten the privacy of users if safeguards were not established.[13]

8. These risks included the "danger similar to wiretapping," of "misuse and interception of 'private' information" during transmission to the central servers, as well as the insecurity of data once it arrived at the central servers.[14]

9. The Cable Communications Policy Act was enacted in 1984 to combat these risks.[15]

---

[9] *Samsung Smart TV - TV Has Never Been This Smart*, SAMSUNG, http://www.samsung.com/us/experience/smart-tv/ (last visited Feb. 10, 2015).

[10] *See* William J. Broad, *U.S. Counts on Computer Edge in Race for Advanced TV*, N.Y. Times (Nov. 28, 1989), http://www.nytimes.com/1989/11/28/science/us-counts-o-computer-edge-in-the-race-for-advanced-tv.html ("Finally, scientists say, the advent of digital television will aid the merging of computers and television, with the prospect of a rush of combined uses.").

[11] David A. Bode, *Interactive Cable Television: Privacy Legislation*, 19 Gonz. L. Rev. 725 (1984).

[12] *See* Rachel Powell, *Tech Notes; Televised Give and Take*, N.Y. Times (Apr. 25, 1993), http://www.nytimes.com/1993/04/25/business/tech-notes-televised-give-and-take.html ("Such capabilities require microprocessors atop the television set and high-capacity fiber-optic lines that link the TV with the cable company -- equipment that is far more sophisticated than the set-top converter boxes and copper cable widely used today. . . .").

[13] *See,e. g.,* David Flaherty, *Protecting Privacy in Two Way Electronic Services,* Communications Library (1985).

[14] Bode, *supra* 13 at 711. *See also Cable Television Privacy Act: Protecting Privacy Interestsfrom Emerging Cable TV Technology,* 35 Fed. Com. L.J. 71, 79 (1983).

10. The Act ensures that cable operators collect only the user data needed to operate the service, keep the data secure while it is in use, and delete the data once it has served its purpose. It also gives cable consumers the right of access to their data.[16]

11. According to the Senate Committee on Commerce, Science, and Transportation, "the development of new and diversified services over interactive two-way cable systems should not impact adversely upon the privacy of the individual."[17]

12. The FTC Chair has recently addressed the specific problem of consumer devices that spy on consumers. Chair Ramirez stated, "Reasonable limits on data collection and data retention is the first line of defense for consumer privacy."[18]

B. Samsung Sells TVs that Record Voice Communications in the United States

13. Beginning in 2012, some companies developed techniques to monitor and record voice communications..[19]

14. Samsung first announced such a television at the Consumer Electronic Expo in 2012.[20]

15. Samsung's "Smart Touch" remote control has a built-in microphone for voice recording; other models include a camera and additional microphones to record voice and hand gesture.[21]

16. As of 2013, Samsung had nearly a thirty percent share of the "Smart TV" market.[22]

---

[15] Cable Communications Policy Act of 1984, 47 U.S.C. §§ 601-639.
[16] *Id* at §631.
[17] S.Rep. No. 67, 98th Cong., 1st Sess. 27 (1983).
[18] [COMPLETE CITE] http://www.usnews.com/news/articles/2015/01/06/the-internet-of-things-ftc-chairwoman-calls-for-tech-privacy-at-ces
[19] *See* Natasha Singer, *The Human Voice, as Game Changer*, N.Y. Times (Mar. 31, 2012), http://www.nytimes.com/2012/04/01/technology/nuance-communications-wants-a-world-of-voice-recognition.html ("Here, Mr. Sejnoha, the company's chief technology officer, and other executives are plotting a voice-enabled future where human speech brings responses from not only smartphones and televisions, cars and computers, but also coffee makers, refrigerators, thermostats, alarm systems and other smart devices and appliances.") -
[20] *See* Christina Bonnington, *Samsung Smart TV 2.0 Can 'Listen, See and Do'*, Wired (Jan. 9, 2012), http://www.wired.com/2012/01/samsung-smart-tvs-ultrabooks/ ("That means you'll be able to toss your remote aside and control your TV using your voice or hand gestures, or perhaps a little help from your Android device. Cooler still, you'll be able to log in to your television using facial recognition, and a service called Family Story will let you show photos, memos and videos from your mobile device.").
[21] *See* Casey Johnston, *Hands-on: Gesture, Voice, and the Many Inputs of Samsung's Smart TV*, ArsTechnica (Mar. 6, 2012), http://arstechnica.com/gadgets/2012/03/hands-on-gesture-voice-and-the-many-inputs-of-samsungs-smart-tv/.

17. SmartTV sales reached more than 90 million worldwide in 2013, and is expected to grow to 228 million by 2018.[23] Other market forecasts estimate that Smart TV sales will reach 141 million in 2015.[24]

18. Samsung has recently purchased LoopPay, a mobile payment processing software company.[25]

19. With the purchase of LoopPay, Samsung announced its intent to compete in the mobile payment services market.[26]

B. Samsung Routinely Intercepts and Records Private Conversations in the Home

20. When the voice recognition feature is enabled, everything a user says in front of the Samsung SmartTV is recorded and transmitted over the internet to a third party regardless of whether it is related to the provision of the service.[27]

21. Under the heading "Voice Recognition" on the company's Privacy Policy page, the company states:

> To provide you the Voice Recognition feature, some voice commands may be transmitted (along with information about your device, including device identifiers) to a third-party service that converts speech to text or to the extent necessary to provide the Voice Recognition features to you. In addition, Samsung may collect and your device may capture voice commands and associated texts so that we can provide you with Voice Recognition features and evaluate and improve the features. *Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition*.[28]

---

[22] *See* Alex Tretbar, *Samsung is Still King of (Smart) TV Sales, But Vizio Eyes the Throne from Second Place*, Digital Trends (Mar. 11, 2014), http://www.digitaltrends.com/home-theater/samsung-and-vizio-ruled-tv-sales-last-year/.
[23] *Smart TV Sales Skyrocket,* Broadband TV News (Nov. 7, 2014), http://www.broadbandtvnews.com/2014/11/07/smart-tv-sales-skyrocket/.
[24] *See Connected TV Sets: Global Sales Forecast 2011-2015*, Statista (2015), http://www.statista.com/statistics/273674/sales-of-internet-connected-tv-sets-worldwide/.
[25] Jonathan Cheng, *Samsung Makes Move Into Mobile Payments*, Wall Street Journal (Feb. 18, 2015), http://www.wsj.com/articles/samsung-makes-move-into-mobile-payments-1424291445?mod=djemalertTECH
[26] *Id*.
[27] *Id.*
[28] *Id.* (emphasis added).

22. Samsung has identified the third party as Nuance, a voice-to-text recognition company.[29]

23. Samsung attempts to disclaim liability for any third party data privacy or security practices, including Nuance's data privacy and security practices. [30]

24. Under the heading "Third Parties," Samsung states:

> Please note that when you watch a video or access applications or content provided by a third-party, that provider may collect or receive information about your SmartTV (e.g., its IP address and device identifiers), the requested transaction (e.g., your request to buy or rent the video), and your use of the application or service. Samsung is not responsible for these providers' privacy or security practices. You should exercise caution and review the privacy statements applicable to the third-party websites and services you use. [31]

25. Samsung has represented that it encrypts the voice communications it transmits to Nuance.[32]

26. Samsung claims it, "takes consumer privacy very seriously and our products are designed with privacy in mind. We employ industry-standard security safeguards and practices, including data encryption, to secure consumers' personal information and prevent unauthorized collection or use." [33]

27. However, a computer researcher determined that Samsung does not encrypt all the conversations it records and transmits to Nuance.[34]

28. Samsung later conceded that the company does not encrypt all the voice recordings it transmits.[35]

29. Samsung also admitted it has not deployed the software necessary to encrypt plaintext transmissions.[36]

---

[29] Samsung Tomorrow, *Samsung Smart TVs Do Not Monitor Living Room Conversations* (Feb. 10, 2015), http://global.samsungtomorrow.com/samsung-smart-tvs-do-not-monitor-living-room-conversations/.
[30] *Samsung Global Privacy Policy*, *supra* at 23.
[31] *Id*.
[32] Samsung Tomorrow, *supra* at 26.
[33] *Id*.
[34] David Lodge, *Is Your Samsung TV Listening to You?*, Pen Test Partners Blog (Feb. 16, 2015), https://www.pentestpartners.com/blog/is-your-samsung-tv-listening-to-you/.
[35] Leo Kelion, *Samsung's smart TVs fail to encrypt voice commands*, BBC News (Feb. 18, 2015), http://www.bbc.com/news/technology-31523497
[36] *Id.* (Samsung stated, "Our latest Smart TV models are equipped with data encryption and a software update will soon be available for download on other models.")

C. Many Consumers Believed That Samsung's Voice Recognition Technique Did Not Involve Voice Recording or Transmission

30. EPIC has compiled many statements from consumers concerning Samsung's decision to intercept and record private communications in the home.

31. Upon learning that Samsung SmartTVs record and transmit conversations in the home, user Dane Jensen commented, "This is an outrageous invasion of privacy and should be illegal. Actually it is illegal but not being enforced. You are not allowed to spy or record someone without consent. I just bought a Samsung TV and never saw or signed any consent form to be recorded. I never saw anything."[37]

32. User Stephen commented, "This should have to be relayed to the customer prior to purchasing. Shame on Samsung for giving into the governments constant strive to monitor the entire population"[38]

33. User potrzebie commented, "I own two Samsung TVs and a Samsung tablet. If they don't stop this right now, I will never buy another Samsung product, ever. Vote with your wallets people." [39]

34. Twitter user @Jason_Garber commented, "From now on wherever I have business meetings and there is a #Samsung #SmartTV present I will ask for its removal." [40]

35. Twitter user @CSElder commented, "@Samsungtweets i will NEVER buy another Samsung tv thanks to your recording feature. You overstep your bounds. #SamsungFail" [41]

36. User beverly commented, "why is this info sent to third party at all it should just stop at the smart tv processor" [42]

37. User cft6vgy7 commented, "This is why devices like cameras and microphones should always be sold separately from computers, TVs, and other electronics. It may not be as "convenient" for the less tech-savvy, but it will be more secure for

[37] David Goldman, *Your Samsung TV is Eavesdropping on Your Private Conversations*, CNN (Feb. 10, 2015) http://money.cnn.com/2015/02/09/technology/security/samsung-smart-tv-privacy/index.html?section=money_latest.
[38] Joshua Barrie, *Samsung's SmartTV Is 'Spying' on Your Personal Conversations*, Yahoo Tech (Feb. 9, 2015) https://www.yahoo.com/tech/samsungs-smart-tv-is-spying-on-your-personal-110539170794.html.
[39] *See* Alyssa Newcomb, *Samsung Privacy Policy: Watch What You Say Around Your Smart TV*, ABC News (Feb. 9, 2015) http://abcnews.go.com/Technology/samsung-privacy-policy-watch-smart-tv/story?id=28829387.
[40] Jason Garber, Twitter (Feb. 8, 2015) https://twitter.com/Jason_Garber/status/564392204358385664
[41] Chris Elder, Twitter (Feb. 10, 2015) https://twitter.com/CSElder/status/565164952214708225
[42] *See* Barrie, *supra* at 30.

every single consumer. Allow consumers to "opt-in" if they don't mind the security risk; don't force users to have to "opt-out" if they want to preserve their own privacy."[43]

38. User John Manso wrote, "I'm glad this is getting national attention. When I first saw the smart TV's come out, very few were concerned. A device in your living room with a camera, a microphone, and 24 hour access to the internet. What could go wrong here? Uh, everything. Who knows who can hack into all of these with a simple piece of software. Everything can be "hacked". No we don't cook up national threats in our living room but privacy is expected and deserved in one's living room wouldn't you say?"[44]

39. User Craig Cheatham commented:

> There are a couple problems evident here beside the obvious one of spying on our conversations. All of these User Agreements convey all sorts of rights to the company without articulating them in a clear manner to the consumer.
>
> My Sony TV would be neutered if I didn't agree to a laundry list of data harvesting. As far as I can tell, ALL of my media surfing is sent back to the mothership. Any pausing, muting, viewing cable, viewing any of the 300 media content apps the TV provides access to, any music, any devices connected to the TV, any games played on the tv. There is NO way to know what is "shared" or who has access to it. Pile on to that the fact of the huge Sony hack and loss of data. Any Agencies who buy this data could compile a dossier of my habits better than I think I know myself.
>
> […]
>
> This trope of Future Shock is a new societal psychological syndrome, as yet unnamed. It is not really paranoia, it is a response to the unwilling sharing of our personal lives that we are powerless to stop without becoming a tree dwelling Luddite. It is an intrusion into what had been considered private personal space.[45]

B. Many Consumers Believe Samsung's Practices Are Illegal Under Consumer Protection or Wiretap Laws

[43] *See* Hayley Tsukayama, *Samsung: Our televisions aren't secretly eavesdropping on you*, The Washington Post (Feb. 10, 2015) http://www.washingtonpost.com/blogs/the-switch/wp/2015/02/10/samsung-our-televisions-arent-secretly-eavesdropping-on-you/

[44] *See* Damon Beres, *How To Stop Your Smart TV From Eavesdropping On You*, Huffington Post (Feb. 9, 2015) http://www.huffingtonpost.com/2015/02/09/your-samsung-tv-is-spying-on-you_n_6647762.html

[45] *See* Shane Harris, *Your Samsung SmartTV Is Spying on You, Basically*, The Daily Beast (Feb. 5, 2015) http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spying-on-you-basically.html

40. User SGHILL commented, "The real question is: can Nuance (the "third party") be subpoenaed for logs of your home activities for a lawsuit. Given recent developments with phone and vehicle blackbox records, I'd say the answer is yes a subpoena will be upheld."[46]

41. User @nordicgod commented, "sounds like phone tapping, which is a federal crime. Has the FCC arrested anyone at Samsung. Does Samsung have a federal judges permission?"[47]

42. User Dan King posted:

> If someone puts a camera in your abode and records your activities, verbal and physical it is a) voyeurism, b) invasion of privacy, c) (I would suggest) cyber stalking. Are the sellers of Samsung aware of the televisions capabilities? One could argue the sellers of Samsung TV's are selling spyware. I find this whole notion horrific. If we cannot discuss things in the privacy of our own home without being overheard we have truly reached the bottom of the chasm and big brother is here to stay!! I do not believe for a moment that Samsung is the only company doing this.[48]

43. User velox commented, "Nuance Communications already has a corporate officer listed as the "Director of National Security Solutions". The person holding this title is a former(?) NSA officer and a former employee at the ODNI's office in DC."[49]

44. User Roger P. commented, "this is how the Government is going to be tracking you, recording you, ect throught all these "wonderful" devices smart phones, smart t.v, GPS navigators even your car will be a grand listening agent.....its very possable and most likely probable"[50]

45. User Mike Westkamper commented, "Its time to upgrade the bill of rights. 'No person or entity may collect, collate or disseminate and information about any other entity or person without informed consent.'. Violation of this clause shall carry monetary and confinement penalties suitable for any [d]amages caused."[51]

---

[46] *See* Tsukayama, *supra* at 35.
[47] *See* Eyder Peralta, *Samsung's Privacy Policy Warns Customers Their Smart TVs Are Listening*, NPR (Feb. 9, 2015) http://www.npr.org/blogs/thetwo-way/2015/02/09/385001258/samsungs-privacy-policy-warns-customers-their-smart-tvs-are-listening
[48] *See* Beres, *supra* at 38.
[49] *See* Tsukayama, *supra* at 35.
[50] *See* Barrie, *supra* at 30.
[51] Javier E. David, *Shhh, not in front of the TV! Samsung may be eavesdropping on you*, Comment 1843692395, CNBC (Feb. 8, 2015) http://www.cnbc.com/id/102407345#comment-1843692395

46. Commenter A Yahoo Reader posted, “Sounds to me that some company is intentionally stepping one someone's privacy rights. It doesn't matter whether it's a big company or not. It shouldn't be allowed or LEGAL.” [52]

47. User Donald P. commented, “It's called ‘bugging’ and it's illegal. Period.”

48. User JoesTalinTroLl commented, “A lawsuit should be filed immediately against samsung. This is a clear violation of the 4th amendment.” [53]

49. User Gunny posted, “Are people really that damned lazy to key the remote??? This recording BS has to be against existing privacy laws. Hopefully a class action law suit will be filed by an Attorney General.”[54]

50. User Rich commented, “No smart tv for me. got enough cameras and and listening devises all around don't need one in my house. Can you say invasion of privacy? Law suites coming.” [55]

51. User Mike Thorne Smallwood commented, “Time to pass legislation requiring that all smart devices must include manual hard switch interrupts not capable of electronic control that allow users to break radio, video and audio circuitry leads, effectively disabling any possibility of hacking the users system when the feature is manually switched to off.” [56]

52. User Allen Burnett commented:

> Any competent hacker can turn on any camera or microphone on any connected device and see/hear whatever is in range. I'm sure the justice department is trying to acquire (or already has) this capability. I'm giving the whole "wired" society another 10 years before people begin revolting against it. They'll buy older non-GPS cars, remove batteries from cellphones when not being used, pay with cash only, and remove all wireless devices from within their homes and businesses. Too many people's lives are being ruined by having their identity/finances/personal information stolen. The problems with being "wired" will soon outweigh the benefits and people will return to paper currency, talking instead of texting, and encrypting whatever electronic devices they must use.[57]

---

[52] *See* Barrie, *supra* at 30.
[53] *Id*.
[54] *Id*.
[55] *Id*.
[56] *See* Natasha Lomas, *Today in Creepy Privacy Policies, Samsung’s Eavesdropping TV,* Techcrunch (Feb. 8, 2015), http://techcrunch.com/2015/02/08/telescreen/.
[57] *Id*.

F. Privacy Experts Warn That Samsung's "Always-On" Voice Recording Practice is Misleading to Consumers

53. EPIC has reviewed many statements by experts in law, technology, and business practices concerning Samsung's decision to intercept and record private communications in the home

54. Technology journalist Natasha Lomas commented:

> The creepy wording of Samsung's SmartTV privacy policy only serves to pass the buck on risks — and fails to educate the user on how exactly the technology they have paid for works, opting to make them feel uneasy/urge them to self-censor instead. If this privacy policy pleases anyone, it's only going to put smiles on the face of Samsung's legal department. So while the content of the policy comes off as Orwellian, the processes here are more impenetrably Kafka-esque, with unseen layers and players (in the case of the VR in this TV the third party processor is apparently Nuance — which has its own privacy policy that TV users suddenly become subject to if they utilize the on-board voice recognition feature) involved in the processing of the user's data, leaving the person who has actually paid for the device in the dark about what exactly is going on. As more consumer electronics devices are networked and augmented with cloud-services, far greater levels of transparency about data processing will be required from device makers — along with clearly signposted opt-outs and user-controls for cloud-processing — to avoid the people who actually pay for this stuff to end up viewing 'smart' as 'suspicious'.[58]

55. Emma Carr, director of privacy campaign group Big Brother Watch, commented:

> Samsung needs to understand that not everyone wants to be spied on by their TV. It is outrageous that the company has even stated in its own privacy policy that if the TV's owner does decide not to share their private information, then the company may still take the information anyway. This leaves users with no knowledge or control over where your information goes or who has access to it and that is simply unacceptable. Few people would expect a TV to intrude on our privacy, yet this is increasingly becoming the case. As this sort of technology is being made to gather increasing amounts of data about

[58] *Id*.

> us, it is vitally important that people should have to choose to make use of these additional services.[59]

56. Paul Levy, a senior researcher at the Unversity of Brighton, commented:

> Did you recently buy a Samsung smart TV? If you are worried about privacy, you may be wondering how smart that decision was following the manufacturer's warnings that its voice-activated televisions may record personal information – that is, your conversations – and transmit them to a third party. The voice-activated television monitors spoken conversations to listen for commands and transmits them to another firm which performs the voice analysis. Samsung stated that the televisions may even do so when the voice-activation feature is turned off. … But it's endlessly apparent how firms that are evangelical about the need for user data to be accessible to them are nevertheless vague about how they then use it. Terms and conditions are long and bamboozling.[60]

57. Ann Cavoukian, the former Ontario privacy commissioner and current executive director of the Privacy and Big Data Institute at Ryerson University, commented, "With Samsung, it's like all of sudden you have to monitor what you should say in your home — the last bastion of privacy, a place that's supposed to be sacrosanct. Are you kidding me?"[61]

G. Samsung is Violating the Subscriber Privacy Provision in the Cable Act

58. The Subcriber Privacy Provision in the Cable Communications Policy Act ("CCPA") prohibits the collection of "personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned."[62]

59. The CCPA also provides, "a cable operator shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are

---

[59] Alex Hern, *The Guardian Samsung Rejects Concern Over Orwellian Privacy Policy*, The Guardian (Feb. 9, 2015), http://www.theguardian.com/technology/2015/feb/09/samsung-rejects-concern-over-orwellian-privacy-policy (quoting the remarks of Emma Carr).
[60] Paul Levy, *Privacy is fast becoming the real disruptive force in digital technology*, The Conversation (Feb. 11, 2015) http://theconversation.com/privacy-is-fast-becoming-the-real-disruptive-force-in-digital-technology-37244.
[61] Matt Kwong, *Samsung SmartTV an 'absurd' privacy intruder, Ann Cavoukian says*, CBC News (Feb. 10, 2015) http://www.cbc.ca/news/technology/samsung-smarttv-an-absurd-privacy-intruder-ann-cavoukian-says-1.2950982.
[62] 47 U.S.C. § 631(b).

necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator."[63]

60. Samsung does not obtain written or electronic consent to recording the private conversations of people in their homes and transmitting those voice recordings to Nuance.

61. Samsung does not "take such actions as are necessary to prevent unauthorized access" to subscriber information.

62. In fact, Samsung deliberately overcollects information provided by cable subscribers, in contravention to Congress' explicit purpose for passing the subscriber privacy section of the CCPA.

63. Samsung is violating the Cable Communications Policy Act.

H. Samsung's Business Practices Violate the Electronic Communications Privacy Act

64. The Electronic Communications Privacy Act ("ECPA") prohibits the "interception and disclosure of wire, oral, or electronic communications." [64]

65. The statute provides that any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication" or "intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection," violates the Act.

66. The statute's definition of "person" includes "corporations."[65]

67. "Oral communications" include only those face-to-face conversations for which the speakers have a justifiable expectation of privacy.[66]

68. "Wire communications" means "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished

---

[63]

[64] 18 U.S. § 2511(1) (2012). (This part of ECPA was originally enacted as Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. 2510-2520 (1964 ed,)(Supp. IV)).

[65] 18 U.S.C. 2510(6).

[66] 18 U.S.C. 2510(2). *See also US v. Larios*, 593 F.3d 82, 92 (1st Cir. 2010).

or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce." [67]

69. Under a few narrow exemptions, ECPA permits the interception of "oral communications" and "wire communications."[68]

70. No exception permits a company to surreptitiously record private communications in the home.

71. By intercepting and recording private communications in the home, Samsung is violating ECPA.

IV. Legal Analysis

A. The FTC's Section 5 Authority

72. The FTC Act prohibits unfair and deceptive acts and practices, and empowers the Commission to enforce the Act's prohibitions.[69] These powers are described in FTC Policy Statements on Deception[70] and Unfairness.[71]

73. A trade practice is unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[72]

74. The injury must be "substantial."[73] Typically, this involves monetary harm, but may also include "unwarranted health and safety risks."[74] Emotional harm and other "more subjective types of harm" generally do not make a practice unfair.[75] Secondly, the injury "must not be outweighed by an offsetting consumer or

[67] 18 U.S.C. 2510(1).
[68] 18 U.S.C. 2511(1).
[69] *See* 15 U.S.C. § 45 (2010).
[70] Fed. Trade Comm'n, FTC Policy Statement on Deception (1983), available at http://www.ftc.gov/bcp/policystmt/ad-decept.htm [hereinafter FTC Deception Policy].
[71] Fed. Trade Comm'n, FTC Policy Statement on Unfairness (1980), available at http://www.ftc.gov/bcp/policystmt/ad-unfair.htm [hereinafter FTC Unfairness Policy].
[72] 15 U.S.C. § 45(n); *see, e.g.*, *Fed. Trade Comm'n v. Seismic Entertainment Productions, Inc.*, Civ. No. 1:04-CV- 00377 (Nov. 21, 2006) (finding that unauthorized changes to users' computers that affected the functionality of the computers as a result of Seismic's anti-spyware software constituted a "substantial injury without countervailing benefits.").
[73] FTC Unfairness Policy, *supra.*
[74] *Id.*; *see, e.g.*, *Fed. Trade Comm'n v. Information Search, Inc.*, Civ. No. 1:06-cv-01099 (Mar. 9, 2007) ("The invasion of privacy and security resulting from obtaining and selling confidential customer phone records without the consumers' authorization causes substantial harm to consumers and the public, including, but not limited to, endangering the health and safety of consumers.").
[75] FTC Unfairness Policy, *supra.*

competitive benefit that the sales practice also produces."[76] Thus the FTC will not find a practice unfair "unless it is injurious in its net effects."[77] Finally, "the injury must be one which consumers could not reasonably have avoided."[78] This factor is an effort to ensure that consumer decision making still governs the market by limiting the FTC to act in situations where seller behavior "unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking."[79] Sellers may not withhold from consumers important price or performance information, engage in coercion, or unduly influence highly susceptible classes of consumers.[80]

75. An act or practice is deceptive if it involves a representation, omission, or practice that is likely to mislead the consumer acting reasonably under the circumstances, to the consumer's detriment."[81]

76. There are three elements to a deception claim. First, there must be a representation, omission, or practice that is likely to mislead the consumer.[82] The relevant inquiry for this factor is not whether the act or practice actually misled the consumer, but rather whether it is likely to mislead.[83]

77. Second, the act or practice must be considered from the perspective of a reasonable consumer.[84] "The test is whether the consumer's interpretation or reaction is reasonable."[85] The FTC will look at the totality of the act or practice and ask questions such as "how clear is the representation? How conspicuous is any qualifying information? How important is the omitted information? Do other sources for the omitted information exist? How familiar is the public with the product or service?"[86]

78. Finally, the representation, omission, or practice must be material.[87] Essentially, the information must be important to consumers. The relevant question is whether consumers would have chosen another product if the deception had not occurred.[88] Express claims will be presumed material.[89] Materiality is presumed

[76] *Id*.
[77] *Id*.
[78] *Id*.
[79] *Id*.
[80] *Id*.
[81] FTC Deception Policy, *supra*.
[82] FTC Deception Policy, *supra* ; *see, e.g.*, *Fed Trade Comm'n v. Pantron I Corp.*, 33 F.3d 1088 (9th Cir. 1994) (holding that Pantron's representation to consumers that a product was effective at reducing hair loss was materially misleading, because according to studies, the success of the product could only be attributed to a placebo effect, rather than on scientific grounds).
[83] FTC Deception Policy, *supra*.
[84] *Id.*
[85] *Id.*
[86] *Id.*
[87] *Id.*
[88] *Id.*

for claims and omissions involving "health, safety, or other areas with which the reasonable consumer would be concerned."[90]

79. The FTC presumes that an omission is material where "the seller knew, or should have known, that an ordinary consumer would need omitted information to evaluate the product or service, or that the claim was false . . . because the manufacturer intended the information or omission to have an effect."[91]

80. The Commission has previously found that a company may not repurpose user data for a use other than the one for which the user's data was collected without first obtaining the user's "express affirmative consent."[92]

B. The FTC's COPPA Authority

81. The Children's Online Privacy Protection Act ("COPPA") regulates the collection of their children's personal information by operators of online services.[93]

82. The Rule, enforced by the FTC, applies to operators of online services, websites, and apps directed to children under 13 as well as operators of online services, websites and apps serving a general audience.[94]

83. Operators of online services directed to children under 13 must comply with COPPA's requirements.[95]

84. Online service operators with general audiences must comply with COPPA when the operator "has actual knowledge that it is collecting or maintaining personal information from a child."[96]

85. To comply with COPPA, operators must obtain parental consent before collecting children's personal information and data.[97]

86. Chiefly, operators must: "(a) Provide notice on the website or online service of what information it collects from children, how it uses such information, and its disclosure practices for such information; (b) Obtain verifiable parental consent

---

[89] *Id.*
[90] *Id.*
[91] *Cliffdale Associates, Inc.*, 103 F.T.C. 110, 110 (1984).
[92] *In the Matter of Google, Inc.;* FTC File No. 102 3136 (Oct. 13, 2011) (Decision and Order), http://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf.
[93] Federal Trade Commission, Complying with COPPA: Frequently Asked Questions, http://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General Questions (last visited Feb. 11, 2015).
[94] Children's Online Privacy Protection Act, 16 C.F.R. § 312.3 (2013).
[95] *Id.*
[96] *Id.*
[97] *Id.*

prior to any collection, use, and/or disclosure of personal information from children; (c) Provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance . . . "[98]

87. Samsung's supplemental SmartTV privacy policy briefly addresses children's privacy: "SmartTV services may make available educational videos and other content appropriate for children, but we do not knowingly collect any personal information from children under the age of thirteen (13) without parental consent, unless permitted by law. If we learn that a child under the age of thirteen (13) has provided us with personal information, we will delete it in accordance with applicable law." [99]

88. Samsung represents that it complies with the requirements of COPPA because it is an online services operator with a general audience and has no "actual knowledge" of any personal information being collected.

89. Samsung specifically targets some features of the SmartTV to young children. The Hopster Smart TV App "brings preschoolers an extensive catalogue of hundreds of episodes of award-winning TV shows." [100]

90. Samsung has acknowledged that SmartTVs are commonly purchased by families with children under the age of 13.[101]

91. Samsung encourages parents to have their children interact with Samsung's Smart TV.[102]

92. Samsung routinely collects the private communications of young children.

C. Count I: Deceptive Failure to Disclose that Samsung Records and Transmits Private Conversations Through Its SmartTV

93. As described in detail above, users were not typically aware that Samsung SmartTVs would record and transmit over the internet their private conversations.

---

[98] *Id.*

[99] Samsung, Samsung Global Privacy Policy – SmartTV Supplement. https://www.samsung.com/uk/info/privacy-SmartTV.html?CID=AFL-hq-mul-0813-11000170 (last visited Feb. 11, 2015).

[100] Samsung, *Samsung Partners with Hopster to Bring TV and Learning Platform for Children to Smart TV* (Dec. 10, 2014), http://www.samsung.com/uk/news/local/samsung-partners-with-hopster-to-bring-tv-and-learning-platform-for-children-to-smart-tv.

[101] *Id.* ("The addition of Hopster to the Samsung Smart Hub means that families can now enjoy even more great content together at home").

[102] *Id.* ("[R]ecent research show[s] that 71% of parents agree that digital devices and screens allow children to explore and discover new things").

94. As described above, users believe that it is illegal for Samsung to record and transmit over the internet their private conversations.

95. As described above, users are so outraged by Samsung's recording and transmission practices that they are calling for class action lawsuits.

96. As described above, Samsung attempted to calm consumers by assuring them that all recorded transmissions met with data encryption standards.

97. As described above, Samsung in fact transmitted some voice recordings unencrypted, in plaintext.

98. Therefore, Samsung's failure to adequately disclose that this commitment to privacy was subject to reversal constitutes a deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

99. Users could not reasonably avoid being aware of the inadequate disclosures regarding Samsung's practice of recording and transmitting private conversations over the internet.

100. Users could not reasonably avoid being aware of Samsung's failure to encrypt all recorded voice transmissions.

101. The inadequate disclosures are not outweighed by countervailing benefits to consumers or to competition.

102. Samsung' inadequate disclosures constitute deceptive acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a).

D. Count II: Unfair Disclaimer of Liability for Third-Party Data Privacy and Security Practices

103. As described above, Samsung attempts to disclaim liability for the data privacy and security practices of companies to whom it transfers user data it has acquired from consumers.

104. As described above, Samsung transmits the private conversations of SmartTV users to a third-party company.

105. As described above, Samsung's privacy policy did not reveal to consumers the name of the third-party company performing the voice-to-text service.

106. As described above, Samsung proceded to mislead consumers about their use of encryption to transmit recorded conversations.

107. By failing to take responsibility for the privacy and safety of users' recorded conversations, Samsung "unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking."

108. Specifically, Samsung users could not reasonably have anticipated that by using a voice-controlled SmartTV, their private conversations would be transmitted, sometimes unencrypted, to a third party company.

109. The inadequate protections are not outweighed by countervailing benefits to consumers or to competition.

110. Therefore, Samsung's inadequate disclosures constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(n).

E. Count III: Violation of Children's Online Privacy Protection Act

111. As described above, Samsung concedes that it markets its SmartTVs to children under the age of 13.

112. As described above, Samsung routinely records conversation in the home, including children's voices, and transmits these conversations to a third party.

113. By failing to ask parents permission to record, store, and transmit children's voices to a third party, Samsung fails to "[p]rovide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance."

114. Parents cannot reasonably review the personal information that Samsung collects from children in the course of recording users' private conversations in the home.

115. Therefore, Samsung's failure to obtain parental consent for the collection and transmission of children's voices constitutes a violation of COPPA, 16 C.F.R. § 312.3 (2013).

V. Prayer for Investigation and Relief

1. EPIC urges the Commission to investigate Samsung, Inc., and enjoin its unfair and deceptive voice collection and transmission practices.

2. Specifically, EPIC requests the Commission to:

a. Initiate an investigation of Samsung's voice recording and transmission practices;
b. Halt Samsung's interception and recording of private communications in the home;
c. Halt Samsung's practice of transmitting recorded communications to a third-party;
d. Investigate Samsung's violation of the Electronic Communications Privacy Act;
e. Investigate other companies engaged in similar practices, and
f. Provide such other relief as the Commission finds necessary and appropriate.

Respectfully Submitted,

_/s/_____
Marc Rotenberg,
EPIC Executive Director

_/s/_____
Julia Horwitz, Director,
EPIC Consumer Privacy Project

_/s/_____
Brooke Olaussen
EPIC Consumer Protection Fellow

Electronic Privacy Information Center
1718 Connecticut Ave. NW Suite 200
Washington, DC 20009
202-483-1140 (tel)
202-483-1248 (fax)