epic.org

1718 Connecticut Ave NW
Suite 200
Washington DC 20009
USA
+1 202 483 1140 [tel]
+1 202 483 1248 [fax]
www.epic.org

July 10, 2015

Attorney General Loretta Lynch
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

Chairwoman Edith Ramirez
The Federal Trade Commission
600 Pennsylvania Ave., N.W.
Washington, D.C. 20580

Dear Attorney General Lynch and Chairwoman Ramirez:

We write to you regarding the growing number of "always on" consumer devices that surreptitiously record the communications of consumers in their homes and may constitute unlawful surveillance under federal wiretap law. Earlier this year, EPIC filed a detailed complaint with the FTC regarding the Samsung "Smart TV" in which we set out facts to support an investigation by the Commission.[1]

We write now to update you as to related matters, to recommend that the Federal Trade Commission undertake a sector wide investigation of these practices, and also to suggest that the Department of Justice determine whether these devices violate federal wiretap laws that prohibit the unlawful interception of private communications. 18 U.S.C. 2510 *et seq.*

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.[2] We have previously

[1] In the Matter of Samsung Electronics Co., Inc., (2015) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/internet/ftc/Samsung/EPIC-FTC-Samsung.pdf.

[2] *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.

alerted the Department of Justice to commercial activities that may constitute unlawful surveillance. [3]

"Always On" Consumer Devices Are Increasingly Prevalent in the "Internet of Things"

In the past weeks, EPIC has learned that Google's Chromium browser contains code that routinely captures private communications.[4] According to Rick Falkvinge, the founder of Sweden's Pirate party, "Without consent, Google's code had downloaded a black box of code that – according to itself – had turned on the microphone and was actively listening to your room."[5] In a blog post, Google conceded that the browser contained this code.[6] The Chromium browser constantly "listens" to the user using the computer's built-in microphone, and when the user speaks the words "OK Google," Chromium activates a voice-to-text search function. This means that Chromium users are subject to constant voice recording in their private homes, without their permission or even their knowledge. The "OK Google" search function is also installed on Android phones. To activate the feature, users are asked only once to give consent to a voice recording being taken and stored on Google servers each time they use the trigger words.[7]

But Google is not the first company to introduce "always on" voice recording in consumer products. In April 2015, EPIC joined the advocacy group Campaign for a Commercial-Free Childhood in promoting a campaign and petition to protest Mattel's "Hello Barbie."[8] The toy is a WiFi-connected doll with a built-in microphone. Hello Barbie records and transmits children's conversations to Mattel, where they are analyzed to determine "all the child's likes and dislikes."[9] The Campaign for a Commercial-Free Childhood explained that Hello Barbie is "a significant violation of children's privacy... Kids using 'Hello Barbie' won't only be talking to a doll, they'll be talking directly to a toy conglomerate whose only interest in them is financial." Moreover, the doll will introduce "always on" voice recording into not only private homes, but specifically into the play of young children.[10]

---

[3] Letter from EPIC to Attorney General Eric Holder, (Apr. 17, 2012) (urging the Justice Department to investigate Google's collection of Wi-Fi data from residential Wi-Fi networks), https://epic.org/privacy/streetview/EPIC-Google-SV-Ltr-DOJ-4-17-12.pdf.

[4] *Google eavesdropping tool installed on computers without permission*, The Guardian (Jun. 23, 2015), http://www.theguardian.com/technology/2015/jun/23/google-eavesdropping-tool-installed-computers-without-permission.

[5] Rick Falkvinge, *Google Chrome Listening In To Your Room Shows The Importance Of Privacy Defense In Depth,* Privacy News Online (Jun. 18, 2015), https://www.privateinternetaccess.com/blog/2015/06/google-chrome-listening-in-to-your-room-shows-the-importance-of-privacy-defense-in-depth/

[6] mgiuca@chromium.org, *Issue 500922: Hotword behaviour in chromium v43 (binary blob download)*, Google Code (Jun. 17, 2015) https://code.google.com/p/chromium/issues/detail?id=500922#c6

[7] Marie Brewis, *How to use OK Google: Android's digital assistant that's more useful than you think,* pcadvisor.co.uk (July 7 2015) http://www.pcadvisor.co.uk/how-to/google-android/how-use-ok-google-from-any-screen-in-uk-3535224/

[8] Campaign for a Commercial-Free Childhood, *Stop Mattel's "Hello Barbie" Eavesdropping Doll*, (Feb. 2015) http://www.commercialfreechildhood.org/action/shut-down-hello-barbie.

[9] Iain Thomson, *Hello Barbie: Hang on, this Wi-Fi doll records your child's voice? What could possibly go wrong?* The Register (Feb. 19, 2015), http://www.theregister.co.uk/2015/02/19/hello_barbie/

[10] *Id. supra* note 5.

Similarly, Samsung's internet-connected "SmartTV "has an "always on" built-in microphone that routinely intercepts and records the private communications of consumers in their homes.[11] 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.[12] Samsung has conceded that it does not encrypt all of the communications it sends to its third party voice-to-text processor.[13] Many consumers were shocked and in disbelief that Samsung's SmartTV voice recognition software involves recording and transmitting their personal communications.[14] EPIC's complaint to the FTC regarding Samsung's "always on" SmartTV charges Samsung with misleading consumers as to the extent of personal information its device collects and transmits, violating the FTC Act, the Children's Online Privacy Protection Act, The Cable Act, and the Electronic Communications Privacy Act.[15]

Microsoft's "always on" voice and motion recorder, called Kinect, is now installed in its Xbox videogame consoles.[16] The Kinect sensor tracks and records users' voice and hand gestures when users say the word "Xbox" followed by various permissible command options.[17] For example, users may turn on their Xbox console by saying, "Xbox on."[18] In order to accomplish this, the Xbox console monitors conversations taking place around it, even when Xbox is turned off.[19] The Xbox console can also register users' faces using the Xbox camera as well as record users' facial expressions and biometric data such as heartbeat rate.[20]

Amazon's voice-activated computer program, "Alexa" is becoming increasingly prominent in the consumer marketplace. Amazon has deployed its Alexa "always on" voice recognition software in its own internet-connected devices, and has made the Alexa voice recognition software available to third party developers to use on their own internet-connected devices.[21] Alexa-enabled products listen for the word "Alexa," which triggers the device to record and send the recording to Amazon's cloud-based servers for processing and storage.[22]

---

[11] Darren Orf, *Samsung's SmartTV Privacy Policy Raises Accusations of Digital Spying,* Gizmodo (Feb. 8, 2015) http://gizmodo.com/samsungs-smart-tv-privacy-policy-raises-accusations-of-1684534051; *See In re Samsung SmartTV,* (2015) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/internet/ftc/Samsung/EPIC-FTC-Samsung.pdf.

[12] *Samsung Privacy Policy – SmartTV Supplement*, Samsung, http://samsung.com/sg/info/privacy/smarttv.html (last visited July 7, 2015, 4:55pm).

[13] Leo Kelion, Samsung's smart TVs fail to encrypt voice commands, BBC News (Feb. 18, 2015), http://www.bbc.com/news/technology-31523497.

[14] *See In re Samsung SmartTV,* (EPIC Complaint) at 7.

[15] *See In re Samsung SmartTV,* (EPIC Complaint) at 17-19.

[16] T.C. Sottek, *The Xbox One will always be listening to you, in your own home (update)*, The Verge (May 21, 2013), http://www.theverge.com/2013/5/21/4352596/the-xbox-one-is-always-listening.

[17] *Kinect and Xbox One Privacy FAQ,* Xbox, http://www.xbox.com/en-US/legal/privacyandonlinesafety (last visited July 7, 2015, 5:16pm).

[18] *Id.*

[19] *See* T.C. Sottek, *supra* note 16.

[20] *Kinect and Xbox One Privacy FAQ, supra* note 17.

[21] Darrell Etherington, *Amazon Unbundles Alexa Virtual Assistant From Echo with New Dev Tools,* TechCrunch (June 25, 2015), http://techcrunch.com/2015/06/25/amazon-unbundles-alexa-virtual-assistant-from-echo-with-new-dev-tools/.

[22] Amazon, *Amazon Introduces the Alexa Skills Kit – A Free SDK for Developers*, Business Wire (June 25, 2015), http://www.businesswire.com/news/home/20150625005699/en/.

Amazon has not disclosed the parameters of the company's data collection practices. A range of companies – including manufacturers of home security systems, toys, and health trackers - are in the middle of incorporating Alexa into their internet-connected devices.[23] Amazon has not disclosed the extent to which the company will have access to the data collected by these third-party devices.

Nest Labs, a company owned by Google, is the manufacturer of internet-connected thermostats, smoke detectors, and security cameras targeted to home owners. The "Nest Cam" is equipped with a microphone, and streams video and sound to a consumer's smart phone in real time.[24] Nest also records and stores 30 days of the footage that it collects from inside the homes of consumers.[25] Nest also offers consumers an alert system which is activated when an "unusual sound" is detected. Nest claims that the "Nest Cam" device is capable of distinguishing between "ordinary background noise" and "unusual noise," such as the "voice of an intruder".[26] Nest has conceded that the company analyses recorded conversations in the home.[27] However, Nest has not clarified how its devices distinguish between unknown and known voices, or how much information the company analyses about a householder's speech in order to do so. All of the data acquired from Nest devices, resides on remote servers, operated and controlled by the company.

Similarly, Canary Connect, another manufacturer of internet-connected home security systems, collects both video and audio recordings from inside the consumer's home. Canary stored these recordings for 90 days.[28] Canary devices can be set to one of three modes - "armed", "disarmed" and "privacy". Unless the device is set to "privacy," the device will record automatically when triggered by motion.[29] However, many users have reported difficulty in determining which mode the device is set to, especially given that the mobile application interface does not notify the user when the device has changed modes – for example, from "privacy" to "armed." [30]

The Commissions and the Department of Justice Should Conduct a Joint Workshop on "Always On" Consumer Devices

Americans do not expect that the devices in their homes will persistently record everything they say. By introducing "always on" voice recording into ordinary consumer

[23] Chris Davies, *Amazon Echo Adds SDK as Alexa Spreads to Other Gadgets*, SlashGear (June 25, 2015), http://www.slashgear.com/amazon-echo-adds-sdk-as-alexa-spreads-to-other-gadgets-25390536/.
[24] Say Hello to Nest Cam, NEST.COM (July 7, 2015) https://nest.com/blog/2015/06/17/say-hello-to-nest-cam/
[25] Samuel Gibbs, Google's new Nest Cam is always watching, if you let it into your home (July 7, 2015) http://www.theguardian.com/technology/2015/jun/18/googles-nest-cam-always-watching-live-streaming-video
[26] Meet Nest Cam, NEST.COM (July 7, 2015) https://nest.com/camera/meet-nest-cam/
[27] How does Nest Aware improve Nest Cam's sound and motion detection? NEST.COM (July 7, 2015) https://nest.com/support/article/How-does-Nest-Aware-improve-Nest-Cam-s-sound-and-motion-detection
[28] Canary Home Security System Review, peaceofhouse.com (July 7, 2015) http://peaceofhouse.com/canary-home-security-system-review/
[29] Michael Brown, Canary review: A sophisticated home-security system packed inside a camera, TECHHIVE (July 7, 2015) http://www.techhive.com/article/2933340/canary-review-a-sophisticated-home-security-system-packed-inside-a-camera.html
[30] *Id.*

products such as computers, televisions, and toys, companies are listening to consumers in their most private spaces. It is unreasonable to expect consumers to monitor their every word in front of their home electronics. It is also genuinely creepy.[31]

The Federal Trade Commission should undertake a comprehensive investigation of "always on" technologies, including those used by Google, Samsung, Nest, Canary, Microsoft, Amazon, and Mattel.

We therefore urge the Federal Trade Commission and the Department of Justic to conduct a joint workshop on "Privacy and Law: The Implications of 'Always-On' Consumer Devices," in order to address the questions and concerns of those whose personal interactions in their homes may be subject to routine surveillance as a result of their engagement with technology.

The agencies should consider a broad range of "always on" consumer privacy issues, including but not limited to:

1. How do "always on" consumer devices operate? When does voice capture occur? Is there an "intercept" of communications? Are communications stored? If so, does the storage occur on the device under the control of the consumer or is the communication transferred to the service provider or a third party? Under what circumstances may these communications be disclosed to others? What security measures are in place to protect this information from improper use?

2. Do companies use "always on" device to authenticate consumers? If so, are the consumer aware of this practice? What security measures are in place to prevent this misuse of authentication features, such as voiceprints?

3. Do companies have an obligation to encrypt the data associated with these services while in transit and when stored? If so, do they in fact encrypt the data?

4. Do companies have to delete data once the voice processing has occurred? If do, they in fact delete the communications they have obtained?

5. Which laws currently regulate surreptitious recording within the home?

6. Is the use of "always on" devices that intercept communications permissible under the federal wiretap act or various state laws? Have consumers given meaningful consent to the interception and recording of their communications? If the purchaser of the device has given consent, does that consent include others in the home whose communications may be recorded and processed?

[31] *See, e.g.,* Stanley Kubrick, "2001: A Space Odyssey" (1968) (HAL 9000: "I'm sorry Dave, I'm afraid I can't do that"), https://www.youtube.com/watch?v=ARJ8cAGm6JE

Thank you for your consideration of this request. We look forward to working with you on this important undertaking.

Respectfully Submitted,

Marc Rotenberg,
EPIC Executive Director

Julia Horwitz,
Director, EPIC Consumer Privacy Project

Alan Butler,
EPIC Senior Counsel

Cc: Sen. John Thune and Sen. Bill Nelson,
U.S. Senate Committee on Commerce, Science, and Transportation

Rep. Fred Upton and Rep. Frank Pallone, Jr.,
U.S. House of Representatives Committee on Energy and Commerce

Sen. Chuck Grassley and Sen. Patrick J. Leahy,
U.S. Senate Committee on the Judiciary

Rep. Bob Goodlatte and Rep. John Conyers, Jr.,
U.S. House of Representatives Judiciary Committee

Marty J. Jackley, Esq.
National Association of Attorneys General