

**UNITED STATES OF AMERICA  
BEFORE THE FEDERAL TRADE COMMISSION**

**COMMISSIONERS: Maureen K. Ohlhausen, Acting Chairman  
Terrell McSweeney**

	)	
<i>In the Matter of</i>	)	
	)	
<b>TURN INC.,</b>	)	<b>DOCKET NO. C-4612</b>
<b>a corporation.</b>	)	
	)	
	)	

**COMPLAINT**

The Federal Trade Commission (“Commission”), having reason to believe that Turn Inc., a corporation, has violated provisions of the Federal Trade Commission Act (“FTC Act”), and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Turn Inc. (“Turn” or “Respondent”) is a privately owned Delaware corporation with its principal office or place of business at 901 Marshall Street, Ste. 200, Redwood City, CA 94063.
2. The acts and practices of Respondent as alleged in this complaint have been in or affecting commerce, as “commerce” is described in Section 4 of the FTC Act.

**RESPONDENT’S BUSINESS PRACTICES**

3. Respondent is a digital advertising company that enables commercial brands and ad agencies to engage in targeted advertising, the practice of using data about a user’s interests in order to deliver online advertising targeted to the user’s interests.
4. Respondent advertises itself to be the “largest independent company in the advertising technology sector,” and states that half of the global online advertising inventory flows through Respondent’s platform. In addition, Respondent claims to reach “over 1.3 billion unique users per month via mobile,” and has “rich profile data on more than 99 percent of North American consumers.”
5. To track consumers across the Web for advertising and other purposes, Respondent uses “cookies” and “web beacons.” “Cookies” are unique, persistent text files stored in a consumer’s browser that allow a company to recognize that unique consumer when the consumer’s browser makes a connection to the company’s servers. Those connections are

sometimes enabled by “web beacons,” which are invisible embedded codes in web pages that instruct the browser to connect to third party services such as Respondent’s. Consumers can delete or otherwise control cookies through settings in their web browsers.

6. To track consumers across mobile apps for advertising and other purposes, Respondent uses device advertising identifiers such as Apple iOS’s Identifier for Advertisers (“IDFA”) and Google’s advertising ID. Device advertising identifiers are useful for targeted advertising companies such as Respondent because many mobile applications cannot set or access browser cookies.

7. Although these device advertising identifiers cannot always be deleted or turned off, consumers concerned about tracking can disassociate themselves from their previous tracking history by resetting the advertising identifier at any time in either Apple’s iOS or Google’s Android settings. In order to ensure that resetting the advertising identifier effectively honors the consumer’s preference, both Apple and Google contractually prohibit application developers from correlating, or syncing, the device advertising identifier with other identifiers, and from allowing third parties obtaining the advertising identifier via the application to do so. Microsoft Windows allows consumers to prevent advertising companies from collecting device advertising identifiers entirely.

8. Beginning in 2013, Respondent began to participate in a Verizon Wireless program that enabled Respondent and its clients to access certain demographic information provided by Verizon Wireless about Verizon Wireless users. To create a shared identifier allowing Verizon Wireless and companies participating in the program to uniquely identify each Verizon Wireless user, Verizon Wireless appended unique identifiers known as tracking headers (“X-UIDH headers”) to its users’ mobile Internet traffic. Verizon Wireless injected these X-UIDH headers into all unencrypted web requests for more than 100 million consumers on the Verizon Wireless data network. During the relevant time period, Verizon Wireless users had no means to prevent the transmission of the X-UIDH header.

9. Between February 2013 and January 2015, Respondent synced the X-UIDH header with other identifiers, including cookies and device advertising identifiers. This practice enabled Respondent to “keep state” on Verizon Wireless consumers – maintaining the linkage between the consumer’s browser or device and an identifier associated with behavioral, demographic, or tracking data – even after a consumer had deleted cookies, reset the device advertising identifier, or both. That is, even if a consumer deleted cookies or reset the device advertising identifier, Respondent would be able to recognize the user by cross-referencing the unique X-UIDH header associated with the device.

10. Respondent’s synchronization with the X-UIDH header also allowed it to recreate unique cookies even after a user had deleted them. In bidding on and delivering online advertising, Respondent was able to constantly synchronize its cookies on a user’s device with the X-UIDH header. If a Verizon Wireless user later deleted her cookies, Respondent would attempt to set a new cookie containing the same unique identifier as the cookie the user had deleted.

11. Until at least April 2015, Respondent’s website included a link to a privacy policy. Respondent’s privacy policy applied both to ads displayed on browsers and within mobile applications. For example, it described its business as providing “relevant, tailored, and privacy-respecting advertisements to consumers viewing a publisher’s properties (*e.g.*, websites, apps, content, etc.)....” (**Exhibit A**, Turn Privacy Guidelines).

12. Until at least April 2015, Respondent’s privacy policy referenced only two tracking technologies: cookies and web beacons. The privacy policy also stated, expressly or by implication, that consumers could prevent Respondent’s tracking by blocking or otherwise limiting cookies:

### **Cookies and web beacons**

Turn uses cookies in connection with our technology. Cookies help Turn better understand the effectiveness of a Turn Ad (for example, by tracking the way in which you may respond to, select and interact with a Turn Ad or any content provided therein, or the site placement and context in which you view a Turn Ad). Turn’s cookies also help control the number of times you view a Turn ad. Most internet browsers automatically accept cookies. You can instruct your browser, by editing in options, to stop accepting cookies or prompt you before accepting a cookie from the websites you visit. If you do not accept cookies, however, you may not be able to enjoy the full functionality of many of the websites you visit.

Turn also uses web beacons, in combination with cookies, to analyze usage patterns. The use of a web beacon allows Turn to record that a particular browser has visited a particular webpage, along with additional Non-PII that the website may choose to include with the beacon.

**Opt out from Tailored but Anonymous Advertising (Turn’s choice mechanism)** If you’d like to opt out of tailored advertising from Turn, please click [here](#) to be taken to our opt out page.

(**Exhibit A**, Turn Privacy Guidelines).

13. Despite the representation that consumers could opt out of tracking by instructing their browser to “stop accepting cookies,” Respondent continued to track consumers by using the Verizon X-UIDH header.

14. Respondent’s opt-out page, linked to its privacy policy, provided instructions on how to opt out of Turn’s tailored advertising. That page provided:

### **Opting out may hurt the sites and apps you love!**

Also, if you opt out, you may be making it harder for your favorite websites or apps to survive. This is because advertisers pay more money to deliver a tailored ad, and your favorite website/app makes more money when they show a tailored ad on their properties. Studies have shown that a significant portion of a

publisher's revenue can come from tailored advertising, and this is particularly true for smaller websites. See 2014 DAA Study and 2010 NAI Study.

SO — if you still want to get ads, but prefer irrelevant ads over tailored ads based on anonymous information and you don't value the free content you enjoy, Turn will place an opt-out cookie on your browser. The opt-out cookie tells our servers not to deliver tailored, anonymous ads to you that deliver high value to the sites and apps you love. If you delete, block, or restrict cookies, or if you use a different computer or Internet browser, you may need to renew your opt-out choice.

(**Exhibit A**, Turn Privacy Guidelines).

15. Through this statement, Respondent conveyed to consumers and to clients evaluating its services that its opt-out mechanism would be effective in blocking tailored, anonymous ads on websites and apps. However, the opt-out cookie applied only to mobile browsers, and was not effective in blocking tailored, anonymous ads on mobile applications.

## **VIOLATIONS OF SECTION 5 OF THE FTC ACT**

### **Count 1: Misrepresentations about Deleting Cookies**

16. As described in paragraph 12, Respondent represented, directly or indirectly, expressly or by implication, that blocking or limiting cookies would restrict Respondent's ability to track consumers.

17. In fact, in many instances, blocking or limiting cookies did not restrict Respondent's ability to track consumers. Respondent continued to track Verizon Wireless customers who had deleted or blocked cookies through the X-UIDH header. Therefore, the representation set forth in paragraph 16 is false or misleading.

### **Count 2: Misrepresentations About Effectiveness of Opt-Out Mechanism**

18. As described in paragraphs 11-14, Respondent represented, directly or indirectly, expressly or by implication, that consumers could opt out of tailored advertising on mobile applications through Respondent's opt-out page.

19. In fact, consumers could not opt out of tailored advertising on mobile applications through Respondent's opt-out page. Therefore, the representation set forth in paragraph 18 is false or misleading.

20. The acts and practices of Respondent as alleged in this complaint constitute deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

**THEREFORE**, the Federal Trade Commission this sixth day of April, 2017, has issued this complaint against Respondent.

By the Commission.

Donald S. Clark  
Secretary

SEAL