

Aleecia M. McDonald
Non-resident Fellow
Stanford Center for Internet & Society

Federal Communications Commission
445 12th St., S.W.
Washington, D.C. 20554

July 5, 2016

Re: WC Docket No. 16-106

I support the proposed rules requiring opt-in consent for ISPs to use the data that transits their systems for advertising. As a privacy scholar typically involved with FTC issues, rather than FCC issues, perhaps I may offer useful background. While co-chairing the Do Not Track standards process we debated opt-in v. opt-out at great length. I am particularly distressed by claims that the FCC would cause confusion by requiring opt-in consent for ISPs while the FTC does not require opt-in consent for “edge” companies.¹ To follow that line of argument to its logical conclusion, that suggests privacy ought never be improved, as any improvement could cause confusion. This is, of course, nonsense. Our current regulations – and often lack thereof – are supposed to set a privacy floor from which companies innovate to create more privacy, not a privacy ceiling that companies are not to exceed. That has been the FTC’s claim all along, complete with hopes that companies would offer more privacy than required;² it is odd to see arguments to the contrary.

Harmonization

The FTC, FCC, and DHS all agree on starting with the Fair Information Practice Principles (FIPs) as a bedrock of privacy thinking. Similarly, the Council of Europe, the OECD, the European Union Data Protective Directive, and the newer European Union Data Protection Regulation are all based around the FIPs. Even the most minimal set of FIPs include notice, choice, access, integrity, and enforcement. I encourage the FCC to continue using FIPs as a tool to guide privacy decisions.

¹ John Eggerton, “Former FTC Chair Has Issues With FCC’s Opt-In CPNI Regime,” *Multichannel News*, (May 11, 2016). <<http://www.multichannel.com/news/fcc/former-ftc-chair-has-issues-fccs-opt-cpni-regime/404836>>

² To quote then-Commissioner Leibowitz, “I write separately to ensure that the Report’s endorsement of self-regulation is viewed neither as a regulatory retreat by the Agency nor an imprimatur for current business practice. [...]Perhaps more companies (even those outside the scope of the behavioral advertising principles) should allow consumers to “opt in” when it comes to collecting their personal information – particularly when the information is “sensitive,” or disclosed to third parties, or collected or shared across various web-based or offline services.” Concurring Statement of Commissioner Jon Leibowitz on FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising <https://www.ftc.gov/sites/default/files/documents/public_statements/concurring-statement-commissioner-jon-leibowitz-ftc-staff-report-self-regulatory-principles-online/p085400behavadleibowitz.pdf>(February 2009).

The EU privacy approach generally requires opt-in consent for most forms of data collection, processing, and data use beyond what the user has requested. Under the General Data Protection Regulation, companies must obtain meaningful consent for additional data processing, with users therefore opting in to targeted advertising. If we are going to discuss harmonizing policies, the FCC would do well to note the growing data practices rift between EU and US laws leading to the collapse of Safe Harbor data transfer provisions.³ The FCC's proposed rule is aligned with the Article 29 Working Party guidance for meaningful opt-in consent, which explicitly rejects opt-out in favor of informed consent and an affirmative opt-in to collect data,⁴ and is also consistent with the EU practice of holding ISPs to higher data privacy standards than publishers. Should the FCC back away from requiring an opt-in informed consent for data collection and re-use, it is hard to imagine how EU citizens in the US could ever have their human rights respected. Recall that those rights attach to the person, regardless of location. Further, the US is also signatory to human rights documents requiring privacy for our own citizens.⁵ In my home state of California, privacy is enshrined in our Constitution as part of Article 1, Section 1. If we are to have harmonization as a goal, there are many options to discuss. As the joke goes, the great thing about standards is that there are so very many to choose from.

Prior History

Until relatively recently, common carriers had a good deal. In exchange for not looking in on user data, they avoided intermediary liability and could not be held legally responsible for the data transiting their network. I am at a loss as to why ISPs should be able to access user data at all, even with consent, for purposes other than network management. While I support the proposed rules for opt-in consent as better than opt-out, I think it is a mistake to offer any use of user data to ISPs for advertising, under any conditions. I consider it a policy failure that we are even having this debate at all. The answer should simply be no, no user data for advertising or any other purpose. Wiretap laws are in place with good reason.

ISPs have been attempting to profit from user data for years. In 2008, ISPs partnered with NebuAd to offer "enhanced" ads based on user data with an opt-out system.⁶ NebuAd shut

³ Wendy Davis, "EU Scraps Cross-Border Privacy Agreement, Imperils Thousands Of US Businesses," *MediaPost's Daily Online Examiner* (October 6, 2015). <<http://www.mediapost.com/publications/article/259867/eu-scraps-cross-border-privacy-agreement-imperils.html>>

⁴ Article 29 Data Protection Working Party, Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising, (Adopted December 8, 2011). <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf>

⁵ Article 12 of the Universal Human Rights Declaration: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." The US has also ratified the International Covenant on Civil and Political Rights, which includes Article 17, "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks."

⁶ Nate Anderson, "Charter 'enhances' Internet service with targeted ads," *Ars Technica* <<http://arstechnica.com/uncategorized/2008/05/charter-enhances-internet-service-with-targeted-ads/>> (May 13, 2008).

down in the face of lawsuits, public outcry, and Congressional concern. ISPs have already heard from Congress that there was to be no data user data collection for ads,⁷ yet here we are again.

Failures of Opt-Out Systems

As mentioned, the NebuAd-ISP partnership allowed users to opt out. However, there were several notable problems with their approach including:

- Many ISPs provided limited information to users, at best informing users that terms and conditions had changed without explaining the scale and scope of privacy change. Some ISPs reportedly did not notify users at all.⁸ It turns out to be very difficult to get companies to clearly explain their invisible practices when profits are enhanced by users' lack of knowledge. One ISP even described targeted ads as an "enhanced online experience" similar to "faster Internet speeds."⁹
- While users might reasonably have expected an opt out to stop data from reaching NebuAd, it did not. User data was collected and transferred to NebuAd even with an opt out. An opt out meant the display of targeted ads was suppressed.¹⁰ This does not meet users' privacy preferences for an opt out of data *collection*, not merely use.
- NebuAd implemented their opt out program by setting an opt out cookie. Of course, as soon as users cleared their cookies – as we advise users do for privacy – then the opt out setting was cleared too.
- The total percentage of users to opt out was about 1%.¹¹ As established below, this is dramatically lower than the percentage of users who prefer not to have data collected and used for targeted advertising. A majority of users who wanted to opt out did not, and their privacy preferences were violated by their ISPs.

The data are already in: opt outs for targeted ads for ISPs did not protect user privacy, and did not accord with user preferences for privacy.

One might argue that NebuAd is but one example. As it happens, we have dozens of examples of companies offering opt outs for targeted ads on websites, again via cookies with all of the problems inherent in that approach. Their record is no less dismal. A study found only 11% of users understood that targeted ad opt outs meant data could still be collected and used though

⁷ Congressmen Markey and Barton wrote, "Any service to which a subscriber does not affirmatively subscribe and that can result in the collection of information about the web-related habits and interests of a subscriber [...] raises substantial questions," and requested ISPs pause working with NebuAd pending Congressional investigation. A copy of their letter to Charter Communication's CEO, dated May 16, 2008, is available from <https://www.wired.com/images_blogs/threatlevel/files/letter_charter_comm_privacy.pdf>.

⁸ Nate Anderson, "Congress goes after NebuAd... again," Ars Technica, <<http://arstechnica.com/tech-policy/2008/07/congress-goes-after-nebuad-again/>> (July 15, 2008.)

⁹ Karl Bode, "Charter: Selling Browsing Data Is Like Offering Faster Speeds," DSLReports <<http://www.dslreports.com/shownews/94466>> (May 16, 2008.)

¹⁰ Ryan Singel, "Can Charter Broadband Customers Really Opt-out of Spying? Maybe Not," Wired <<https://www.wired.com/2008/05/theres-no-optin>> (May 16, 2008.)

¹¹ Karl Bode, "Infighting At ISPs Over Using NebuAD," DSLReports, <<http://www.dslreports.com/shownews/Infighting-At-ISPs-Over-Using-NebuAD-94835>> (May 29, 2008.)

targeted ads could not appear, which is the same percentage of users who thought the opt out itself was actually a scam.¹²

Failures of Self-Regulation

There are a few key ways in which ISPs *differ* from other edge companies collecting data. First, due to how very little competition there is in the broadband market, the principle of choice is intrinsically challenging. If a consumer has only a broadband duopoly, it is unlikely that either of the ISPs will voluntarily elect to monetize less user data. Market pressure will create a race to the bottom. Internet users can choose to forgo Google and Facebook while being part of digital life (if barely,) but cannot do away with an Internet provider by very definition.

Second, the FCC has the benefit of acting in 2016 after seeing how very poorly the FTC's self-regulatory approach has served the health of the Internet and society as a whole over the last three decades. The FTC has been consumers' best friend for online privacy, yet users find the state of online privacy to be fairly miserable:

- 91% of adults agree or strongly agree that consumers have lost control of how personal information is collected and used by companies, with only 1% strongly disagreeing.¹³
- While ISPs were not part of their survey, Pew Research found Americans have low confidence in their records remaining private. For email providers, landline, and mobile telephone providers, at most 6% of adults were very confident their records would remain private. Coming in last out of 11 categories, only 1% of adults were very confident that online advertisers would keep their records private.¹⁴
- In a study of web advertisement, about 20% of participants wanted the benefits of targeted advertising, but 64% found the idea invasive. Data collection can cause a chilling effect, with 40% self-reporting they would change their online behavior if they knew advertisers were collecting data and only 15% saying they would not change their online behavior in response to advertisers collecting data.¹⁵

With privacy hard to come by, users often become cynical. As one journalist concluded while reporting on NebuAd, "Online advertising is a \$11 billion (and growing) business, and it's been fairly apparent that the FTC's priority is protecting revenue streams, not consumers."¹⁶ It is hard for companies, and governments, to regain user trust once it is damaged.

¹² A. M. McDonald and L. F. Cranor, Americans' Attitudes About Internet Behavioral Advertising Practices. Proceedings of the 9th Workshop on Privacy in the Electronic Society (WPES) (October 4, 2010.)

¹³ Lee Rainie, "The state of privacy in America: What we learned," Pew Research Blog, <<http://www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacy-in-america/>> (January 20, 2016.)

¹⁴ IBID.

¹⁵ A. M. McDonald and L. F. Cranor, Americans' Attitudes About Internet Behavioral Advertising Practices. Proceedings of the 9th Workshop on Privacy in the Electronic Society (WPES) (October 4, 2010.)

¹⁶ Karl Bode, "Infighting At ISPs Over Using NebuAD," DSLReports, <<http://www.dslreports.com/shownews/Infighting-At-ISPs-Over-Using-NebuAD-94835>> (May 29, 2008.)

With users burdened to opt-out of data collection from edge providers, we are currently locked in an “arms race” between citizens trying to protect their privacy with tools like ad blockers,¹⁷ and companies trying to collect data no matter how many times citizens signal they do not want to be tracked online.¹⁸ This set of measures and counter-measures is a symptom of a deep market failure, complete with examples of a “lemons market” where products die because there is no longer any way to reliably signal a company will respect privacy. As trust evaporates, new entrants suffer, including societally enhancing projects around medical data and the Internet of Things, resulting in decreased innovation and decreased Internet use. Chilling effects are real and measurable, with lower online engagement as a result of privacy concerns.¹⁹ Meanwhile, the ad market is in decline.²⁰ Lack of privacy regulation has caused real and lasting harms on all sides of the market for Internet stakeholders, and works well for very nearly no one.

Encryption is not a Cure

One argument against the FCC’s proposal is that a trend to more encryption means ISPs accessing user data without consent is not a problem.²¹ I find this line of argument inexplicable. Encryption covers a lot of possible approaches and it is not clear just what form of encryption is envisioned. All three approaches to encryption below are expensive, require specialized knowledge, or don’t significantly affect user privacy:

1. Users can prefer encrypted websites, but users have no control over which sites do and do not offer encryption. Many publishers do not offer encryption, in part because most ads are not encrypted. Browser security measures discourage use of encrypted sites that include unencrypted ad content. Further, even if the traffic to individual website pages itself is encrypted, ISPs can track the visits to the websites. It is not clear how encryption would help at all in this case.
2. Users could purchase additional third-party VPN services to encrypt all traffic from their devices (typically costing an additional \$80-\$120 per year per device,) plus need to learn how to set up, configure, and use those VPN services. This is a non-trivial investment.
3. Users could purchase and attempt configure a small-office router (typically \$100-\$200) to create a site-to-site VPN, allowing the user to force all traffic for all devices through

¹⁷ “How Ad Blockers Have Triggered an Arms Race on the Web,” MIT Technology Review <<https://www.technologyreview.com/s/601581/how-ad-blockers-have-triggered-an-arms-race-on-the-web/>> (May 26, 2016.)

¹⁸ For example, with Do Not Track built into browsers starting in 2011, there have been millions of Do Not Track signals ignored over the past half decade.

¹⁹ Rafi Goldberg, “Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities,” National Telecommunications & Information Administration, <<https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities>> (May 13, 2016.)

²⁰ John Herrman, “Media Websites Battle Faltering Ad Revenue and Traffic,” *The New York Times*, <<http://www.nytimes.com/2016/04/18/business/media-websites-battle-falteringad-revenue-and-traffic.html>> (April 17, 2016.)

²¹ Grant Gross, “FCC wants ISPs to get customer permission before sharing personal data,” PC World, <<http://www.pcworld.com/article/3043019/security/fcc-wants-isps-to-get-customer-permission-before-sharing-personal-data.html>> (March 10, 2016.)

the VPN service (again, typically \$80-\$120 per year). Unfortunately, there are currently no available out-of-the-box solutions, so a user attempting this would also need to understand router and network configuration at a level not common outside the networking industry.²²

All of these options require users to take meaningful steps, to learn new ways of using the internet, and potentially to pay substantially more. None of them are known to most users in the first place. Further, ISPs would have incentive to decrease rates of adoption for encryption on websites if they were part of the advertising ecosystem, in order to avoid mixed content warnings. One would rather see ISPs have incentive to promote encryption and security, not undermine both.

On a personal note, my small, local ISP is notably good on privacy. They could provide faster Internet access but that requires transiting a national ISP that has privacy practices I find unacceptable. My household has invested dozens of hours into research and configuration to try to ameliorate issues because we have diminished trust in the national ISP. My household is more technically oriented than most and we are actively struggling with this as a problem. If your threat model includes your ISP, there are no good, usable, consumer-focused solutions on the market at this time.

Most Consumers Do Not Want Targeted Ads

There are also arguments that users want their ISPs to serve ads based on their data. It is likely true that a small percentage of users would prefer to have more relevant ads from their ISPs, as a small percentage of users prefer targeted ads on websites. The majority of users, however, very likely would not. This topic has been studied for nearly a decade, with persistent and stable results that most Americans would prefer not to be profiled and shown targeted ads:

- 57% of respondents are “not comfortable” with browsing history-based behavioral advertising, “even when that information cannot be tied to their names or any other personal information.”²³
- 66% of adults do not want tailored advertising, which increased to 86% when participants were asked about three common techniques used in web advertising.²⁴
- Furthermore, the question at hand is not just about advertising but about ISPs monitoring users’ traffic in new ways. 88% of Americans feel it is important that they not have someone watch or listen to them without their permission, with only 9%

²² As one example configuration file please see <<https://forums.sonic.net/viewtopic.php?f=13&t=3531#p26003>>. To quote the author who generously shared a portion of his 500+ line configuration file, “good luck.”

²³ TRUSTe. “2008 Study: Consumer Attitudes about Behavioral Targeting,” <http://danskprivacynet.files.wordpress.com/2009/02/truste2008_tns_bt_study_summary1.pdf> (March 2008).

²⁴ Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, and Michael Hennessy. “Americans Reject Tailored Advertising and Three Activities that Enable It,” (September 29, 2009.)

believing it is not important.²⁵ Even if ISPs never made a dime from user data, users would still have concerns about a system that collects, classifies, and persists.

Why, then, should we ask the majority of users to jump through the hoops of opting out, when avoiding targeted ads is most users' preference? From an efficiency perspective it makes no sense to ask the majority of users to figure out how to opt out while privileging the small subset of users who actively want ISPs to target ads. Were companies engineering for efficiency, they would build an opt-in database and only maintain data for the smaller subset of users who want to join their new advertising services. An opt-in system is simply more sensible.

The final, and primary, distinction between ISPs and edge providers is that the FCC regulates ISPs. The FCC has the clear authority and obligation to do better than requiring users to opt-out for privacy, and certainly ought not be hamstrung by proven mistakes of the past.

Thank you for your time, and for your work on behalf of the American people.

Aleecia M. McDonald
Non-resident Fellow
Stanford Center for Internet & Society

²⁵ Mary Madden and Lee Rainie, "Americans' Attitudes About Privacy, Security and Surveillance," <<http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>> (May 20, 2015.)