BakerHostetler

Cross-Device Tracking and the Internet of Things

By: Alan Friel and Niloufar Massachi[1]

Gone are the days of single-browser tracking. User behavior has advanced. Enter the era of cross-device tracking – the process of tracking a single consumer across all of the consumer's devices. Both the Federal Trade Commission (FTC) and the Digital Advertising Alliance (DAA), a U.S. advertising industry self-regulatory program, have taken notice, and the practice faces significant hurdles under the new European Union General Data Protection Regulation.[2]

Historically, first (i.e., publishers) and third (e.g., ad tech providers) have used cookies (i.e., code attached to a consumer's web browser) to track consumers online for purposes such as to remember them and their preferences when returning to a site and recognizing their interests on and off of the site to deliver more relevant content or ads. However, cookies are limited in that they do not capture information outside a single browser and do not work in a mobile app environment. With the proliferation of devices and platforms over the past several years, and consumers spending more time across devices,[3] and on mobile apps, companies have needed a means to capture information beyond that of a single browser to effectively conduct analysis, improve consumer experiences, and target relevant content and ads.

At the same time, consumer products are becoming interactive – collecting data useful for marketing and product improvement. This also presents data privacy and protection issues that regulators in the U.S. and abroad are closely watching.

---

[1] Mr. Friel (Afriel@BakerLaw.com) is a partner in the advertising, marketing & digital media and privacy & data protection groups of BakerHostetler. Ms. Massachi is an associate. Both are resident in the Los Angeles office.
[2] EU compliance is beyond the scope of this article. However, as we go to press the current draft of the EU e-Privacy Regulation to be revised under the 2018 GDPR implementation is undergoing revision in an attempt to try to accommodate both the ad industry and privacy advocate and the future of digital advertising in the EU is very much in question.
[3] Cross-Device Trends Roundup (2014), *available at* https://www.emarketer.com/public_media/docs/eMarketer_Cross_Device_Trends_Roundup.pdf

This article will summarize the state of the law in the U.S. and highlight issues for manufacturers and marketers related to tracking and targeting consumers via their communications and other devices and activities.

Cross-device tracking

Cross-device tracking involves linking a wide range of digital or internet-connected devices together in the hopes of tracking a particular household or consumer. Linking is accomplished through one of two methods (and sometimes a combination of both).

The first method – deterministic – ties multiple devices to a persistent identifier, such as an email address, login credential or hashed personally identifiable information. For example, when a consumer logs in to services using social media network credentials (e.g., Facebook Connect) via various devices, the social media network can determine that the consumer's phone, desktop and tablet all belong to the consumer. This enables highly reliable cross-device data collection and user profiling, and creates an advantage for walled-garden platforms and providers that are able to control the persistent identifier.

The second method – probabilistic – makes inferences based on aggregated information passively collected from multiple devices. For example, when a phone and tablet are consistently used in the same location, a company can infer that the phone and tablet belong to the same consumer or household. Various companies have developed "black box" databases running algorithms on big data from multiple sources to attempt to link device identifiers to likely common consumers. This data can then be supplemented with advertiser and ad network databases to further match consumers and their devices and activities.

Information from devices linked to a particular consumer is pooled together into a device graph. Companies may use and share such device graphs for a multitude of reasons, such as to authenticate consumers or for targeted advertising.

On Nov. 16, 2015, the FTC hosted a workshop[4] to address issues specific to cross-device tracking. That same day, the DAA issued its Application of the Self-Regulatory Principles of Transparency and Control to Data

[4] Cross-Device Tracking (2015), *available at* https://www.ftc.gov/news-events/events-calendar/2015/11/cross-device-tracking

Used Across Devices[5] (DAA Guidance) on how its self-regulatory principles apply to cross-device tracking. Companies that engage in, or intend to engage in, cross-device tracking should review the workshop transcript and comments, as well as the DAA Guidance, in order to better understand how the principles of transparency (consumer notice) and control (consumer choice), as applied to cross-device data, are evolving under U.S. legal and self-regulatory privacy schemes.

The FTC workshop

The FTC workshop was an information-gathering exercise carried out by the FTC that involved participation from various panelists, FTC staff and then-Chairwoman Edith Ramirez. While the workshop did not result in FTC guidance, at the end of the workshop, Maneesha Mithal, associate director of the FTC's Division of Privacy and Identity Protection, identified the following five takeaways, which may shed light on the FTC's potentially emerging position on cross-device tracking and warrant consideration by companies that engage in or intend to engage in cross-device tracking:

1. Balance benefits and intrusion. Cross-device tracking has many benefits. Cross-device tracking allows for seamless, consistent consumer experiences across devices and better techniques for protecting consumers from fraud. It also allows for improved ad efficiency, reduced ad fatigue and better monetization practices. At the same time, cross-device tracking raises certain privacy concerns. Chairwoman Ramirez emphasized this point early in the workshop when she explained how cross-device tracking blurs the line between aspects of consumers' lives that they may intend to keep separate. One of the workshop panelists also made this point when he argued that companies, not consumers, seem to benefit most from cross-device tracking.
2. Increase transparency and choice. Companies need to work toward providing greater transparency, choices and education for consumers. In the workshop, several panelists argued that there are few tools that allow consumers to understand which devices are linked to their device graphs. Where such tools do exist, they allow only for opting out of targeted advertising. One panelist suggested that consumers should be able to opt out of entire device graphs using a single opt-out.
3. Avoid the unexpected and sensitive data and uses. Companies should engage consumers in a way that will not cause consumers to lose trust in the marketplace. This point was based on arguments from

[5] Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices (2015), *available at* http://www.aboutads.info/sites/default/files/DAA_Cross-Device_Guidance-Final.pdf

several panelists that although consumers know tracking exists, consumers may not understand the extent of data mining or that anonymous identifiers and hashed personally identifiable information can still be linked to a particular consumer. Furthermore, consumers may not expect that sensitive data could be derived from pieces of data that are not traditionally sensitive (e.g., websites visited). One panelist in particular argued that as data sets become more easily cross-referenceable and aggregable, the distinction between personally identifiable information and non-personally identifiable information may diminish.

4. Design to minimize impact. There is room for companies to improve transparency and innovate through new ideas -- essentially privacy-by-design.[6] As Chairwoman Ramirez emphasized early in the workshop, data minimization policies and technologies will become more important as device graphs increase in size.
5. Provide meaningful disclosures that are clear, complete and reflective of actual practices. Companies should be mindful of the representations they make. Ms. Mithal specifically pointed out that companies risk violating Section 5 of the FTC Act (prohibiting deception or unfairness in commerce) if they provide opt-outs that are unclear or deceptive, or that conflict with consumer expectations. The same applies to publishers that describe third-party opt-out programs in their privacy policies.

Synthesizing these five takeaways articulated by the FTC staffer, the chief lesson is that companies, now more than ever, need to be aware of the data collection activities associated with their services, including those conducted by third parties on their services, and know that the FTC is closely monitoring cross-device tracking for deceptive or unfair practices. As discussed in the Internet of Things section below, the FTC under the last administration started to apply unfairness jurisdiction to information collection a consumer would not reasonably expect, and suggested that such informational invasion might create a cognizable harm not outweighed by benefits to consumers or competition. While the new Republican acting chairperson has been much less hawkish on the issue, the FTC has scheduled workshops in late 2017 and early 2018 on the issue of information injury. Regardless of where U.S. regulators may land on the issue, by applying privacy by design, companies can be aware of the data collection and use that they and third parties are doing in connection with

[6] Privacy by Design (PbD) is a methodology of incorporating Fair Information Practices (FIPs) principles adopted by regulators worldwide into the product development process. Conceived of by Ontario, Canada Information & Privacy Commissioner Ann Cavouskian, PbD has been adopted or recommended by privacy regulators in the US and abroad, including the E.U. For more information, see www.privacybydesign.ca.

their products and consumers, and apply principles of data minimization and consumer notice and choice to avoid regulatory scrutiny and potential consumer backlash.

Furthermore, companies can look to how the FTC has applied its Section 5 authority to traditional browser-based tracking to cross-device tracking. These cases can be broken into standing for four privacy principles that will be applicable to cross-device tracking and targeting:

1) Effective notice, which may need to be enhanced for unexpected tracking.

Upromise Inc. settled[7] with the FTC regarding charges that it engaged in the deceptive practice of collecting consumers' personal information through a web-browser toolbar without disclosing to consumers the scope of information it was gathering. Pursuant to the settlement order, Upromise must obtain consumers' consent to install the web-browser toolbar and clearly disclose to consumers the data collection practices it engages in.[8]

Earlier the FTC filed complaints against other companies alleging deception where online data collection and use privacy practices were alleged not to have been adequately disclosed to consumers. For instance, in one, the scope of its tracking software's data collection was alleged not to be in a sufficiently clear and conspicuous manner. Although the company disclosed to consumers that its software would track consumers' online browsing, and even paid consumers for their consent, it did not disclose that the software would monitor online secure sessions, such as online bank statements and video rental records until the consumer worked through several click throughs to get deeper and deeper into a set of online terms. The FTC applied advertising disclosure effectiveness principles to find the disclosures inadequately given.[9] Thereafter, advertising disclosure principles have been applied to data privacy and security disclosures

These cases stand for the proposition that not only must all material data collection and use practices be disclosed, but they the disclosure must be done in an effective manner. The more unexpected the practice, the

[7] USA v. Upromise, Inc., Stipulated Order, *available at* https://www.ftc.gov/system/files/documents/cases/upromise_order_-_3-23-17.pdf

[8] Membership Reward Service Aimed at College Savers Settles FTC Charges That Its 'TurboSaver Toolbar' Feature Deceptively Collected Consumers' Personal Information (2012), *available at* https://www.ftc.gov/news-events/press-releases/2012/01/membership-reward-service-aimed-college-savers-settles-ftc

[9] For more information, review the FTC's 4 P's guidance – Prominence, Presentation, Placement and Proximity – to effective disclosures. See, e.g., https://www.ftc.gov/news-events/blogs/business-blog/2014/09/full-disclosure.

greater the need to enhance the disclosures through proximity, presentation, placement and prominence at the point of collection or user interactivity.

2) Sensitive data collection requires express consent.

The FTC filed a complaint[10] against Goldenshores Technologies LLC, the creator of a flash light app for Android mobile devices, alleging that the company engaged in deceptive acts by not effectively disclosing that consumers' geolocation information would be collected and shared with third parties for location-based advertising, and by offering consumers an option to not share their information where the information was already being automatically shared. The FTC found location data to be sensitive and in the context of a flashlight, unexpected. Per a settlement[11] agreement with the FTC, going forward the company cannot misrepresent how it collects and shares consumer information and must obtain consumer consent before collecting and sharing consumers' geo-location information.

Vizio settled[12] charges with the FTC regarding allegations that it used software in its televisions to collect information on what consumers watch without the consumers' consent. Noting that the Cable Act protects the privacy of TV viewing by those most likely to have access to that information – TV services distributors, the FTC concluded that consumers would have a privacy expectation as to their viewing, which the commission also assumed could be sensitive, and that collection by a TV monitor manufacturer would be unexpected. The FTC found the disclosures of the tracking and data sharing to be inadequate, and as discussed further in the next section, the majority of the commission went so far to say the data practices as conducted were unfair. Pursuant to the settlement and consent order, Vizio had to destroy the data and change its transparency and choice practices to meet FTC guidance standards and additional best practices.

The Massachusetts attorney general (AG) recently took preemptive action against an ad tech company that had used geoaware/geofencing technology to send pro-life/anti-choice ads to users of mobile phones that were

[10] In the Matter of Goldenshores, Complaint, *available at* https://www.ftc.gov/system/files/documents/cases/140409goldenshorescmpt.pdf
[11] In the Matter of Goldenshores, *available at* https://www.ftc.gov/system/files/documents/cases/140409goldenshoresdo.pdf
[12] Vizio Settlement: Smart TVs should not track your shows without your O.K. (2017), *available at* https://www.consumer.ftc.gov/blog/2017/02/vizio-settlement-smart-tvs-should-not-track-your-shows-without-your-ok

proximate to abortion clinics. The AG obtained a commitment[13] from the company not to send ads based on sensitive data to Massachusetts residents without clear and express prior consent.

3) Opt-outs must be effective.

The FTC filed a complaint[14] against Chitika Inc., a company that enables online behavioral advertising, alleging that it engaged in deceptive acts and practices by representing to consumers that when they opt out of targeted advertising, such an opt out will be essentially persistent when in fact the opt-out cookies were set to expire after 10 days. Per the negotiated consent order,[15] Chitika must provide consumers an opt-out tool that enables opt-out with no more than one click and maintains the consumers' opt-out setting for at least five years.

It its complaint[16] against ScanScout, an online advertiser, the FTC alleged that the company deceptively claimed that consumers can change their browser setting to opt out of getting targeted ads when in fact changing browser settings did not block targeted ads because the company used Flash cookies, which reside locally on a computer and are not like traditional cookies browser-based. Per a settlement[17] with the FTC, ScanScout cannot misrepresent information regarding how it collects data or regarding whether and how consumers can control data collection.

---

[13] AG Reaches Settlement with Advertising Company Prohibiting Geofencing Around Massachusetts Healthcare Facilities (2017), *available at* http://www.mass.gov/ago/news-and-updates/press-releases/2017/2017-04-04-copley-advertising-geofencing.html
[14] In the Matter of Chitika, Inc., Complaint, *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/06/110617chitikacmpt.pdf
[15] In the Matter of Chitika, Inc., Decision and Order, *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/06/110617chitikado.pdf
[16] In the Matter of ScanScout, *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/12/111221scanscoutcmpt.pdf
[17] In the Matter of ScanScout, *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/12/111221scanscoutdo.pdf

The FTC filed a complaint[18] against Google Inc. alleging that the company misrepresented to users that they effectively opt out of Google's advertising tracking cookie if they do not change their browser settings. To settle[19] the charges, Google agreed to pay a record $22.5 million civil penalty.

4) Adhere to your privacy promises.

In a complaint[20] against Epic Marketplace Inc., the FTC alleged Epic secretly determined whether consumers had visited certain domains using "history sniffing." Epic's privacy policy claimed that it was merely tracking user visits to Epic's network sites, but despite the promises in its privacy policy, in reality Epic allegedly collected information regarding users' browser history from other sites to deliver advertisements. Per a settlement agreement with the FTC, Epic will no longer engage in history sniffing and can no longer misrepresent information regarding how it collects and shares data or regarding the scope of its software's ability to determine whether a user has visited a website.

The FTC filed a complaint against Nomi Technologies, a company that provides retailers with in-store analytics using sensor-based tracking of consumers' mobile devices, alleging that it falsely promised consumers they can opt out at stores using its services. An FTC order[21] prohibits Nomi from misrepresenting its privacy practices in the future.

These same four principles can be expected to be applied to the FTC's deception enforcement regarding cross-device tracking, even if this commission puts the brakes on unfairness claims.

DAA Guidance

The advertising industry has issued its own self-regulatory principles on cross-device data, timed to correspond with the original 2015 FTC workshop. The DAA Guidance applies the DAA's existing principles of

---

[18] USA v. Google, Inc., *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809googlecmptexhibits.pdf
[19] USA v. Google, Inc., *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809googlestip.pdf
[20] In the Matter of Epic, Inc., *available at* https://www.ftc.gov/sites/default/files/documents/cases/2013/03/130315epicmarketplacecmpt.pdf
[21] In the Matter of Nomi, Inc., *available at* https://www.ftc.gov/system/files/documents/cases/150902nomitechdo.pdf

transparency and control for interest-based advertising[22] to cross-device data, and most of the U.S. advertising ecosystem falls within its jurisdiction. Compliance is often contractually required by and amongst advertisers, ad agencies, ad networks and publishers. DAA participants are expected to publicly commit to compliance within its principles, making failure to comply a false advertising statement the FTC and state regulators can prosecute as a deceptive practice.

The DAA Guidance provides for notice obligations regarding the collection of multi-site data[23] and/or cross-app data[24] for both first parties (i.e., the site, app or service on which data is collected) and third parties (i.e., a party other than the site, app or service operator that collects such data on an unaffiliated site, app or service). In addition, the DAA has made clear that for uses other than certain excepted uses (e.g., intellectual property protection, consumer safety, research, authentication) including, specifically, interest-based advertising, participants must provide a consumer opt-out, which could be accomplished through the DAA-administered AdChoices[25] and AppChoices[26] programs, and transparently give notice of such choice mechanism.

Takeaway

With the expansion of multi-device consumer behavior, cross-device tracking and targeting is certain to become increasingly common. The degree of consumer notice and choice required for that activity, and various uses of the data collected, is evolving and U.S. regulators are starting to sound frighteningly European in their approach to the issue of consumer privacy as it relates to data collection that is so complex and in the background that typical consumers may not expect it.

For more information on cross-device tracking, please see our blog post here.[27]

---

[22] For more information see www.aboutads.info/principles and www.asrcreviews.org/accountability-program-decisions/.
[23] Self-Regulatory Principles for Multi-Site Data (2011), *available at* http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf
[24] Application of Self-Regulatory Principles to the Mobile Environment (2013), *available at* http://www.aboutads.info/DAA_Mobile_Guidance.pdf
[25] *Available at* http://youradchoices.com/
[26] *Available at* http://youradchoices.com/appchoices
[27] The FTC and DAA Set Their Sights on Cross-Device Tracking (2015), *available at* https://www.dataprivacymonitor.com/behavioral-advertising/the-ftc-and-daa-set-their-sights-on-cross-device-tracking/

The Internet of Things

The Internet of Things (IoT) refers to consumer devices that are connected, directly or indirectly, to the internet or other internet-connected devices. Today, cars, household appliances, so-called wearables like Fitbits, smart TVs, home-command centers like Nest, Alexa and Google Home, and even sex toys and toothbrushes are collecting consumer data, often of a potentially sensitive nature, and transmitting it over Wi-Fi, Bluetooth and the internet. The same privacy and data security issues that apply to computers and mobile phones apply to the IoT. Given the potentially sensitive nature of the data involved, the first generation of lawsuits and regulatory actions has involved babies, abortions, at-home movie viewing and vibrators. But these cases are not outliers, and there are lessons to be learned for all companies considering a foray into the IoT. And with the public notoriety these cases are generating has come the interest of the FTC, state AGs and legislatures, class action plaintiffs, and consumer advocacy groups.

FTC actions against TRENDnet, Aaron's, D-Link and Lenova

The first IoT FTC action was TRENDnet, when, in September 2013, the maker of babycams that got hacked settled[28] FTC deception and unfairness claims arising out of allegedly unreasonably inadequate security. A month later, the FTC settled[29] with Aaron's Inc., which rented consumers computers equipped with "detective mode" software that was capable of capturing keystrokes and screen shots and activating microphones and cameras. It was alleged that staff used this software not only to recover lost and stolen devices but also to spy on users, including recording their most intimate acts. As part of the negotiated consent decree, Aaron's agreed to give notice at purchase of the software and its capabilities, and to give clear and enhanced activation notice whenever it was used other than in response to a loss or theft report. This past January, the FTC filed a lawsuit[30] against connected camera and home router maker D-Link for unfairness arising out of allegedly

[28] Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Filed to Protect Consumers' Privacy (2013), *available at* https://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles

[29] Aaron's Rent-To-Own Chain Settles FTC Charges That It Enabled Computer Spying by Franchisees (2013), *available at* https://www.ftc.gov/news-events/press-releases/2013/10/aarons-rent-own-chain-settles-ftc-charges-it-enabled-computer

[30] FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras (2017), *available at* https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate

unreasonable security, even though no security breach had yet occurred. This September, Lenovo Inc. settled[31] with the FTC regarding charges[32] that Lenovo sold laptops with preinstalled software that put consumer privacy at risk by enabling potential attackers to capture communications with any website, such as financial institutions. And then there is Vizio….

FTC settles with VIZIO Inc.

In a case with potentially far-reaching implications, the FTC and the New Jersey attorney general settled with Vizio Inc., a consumer electronics manufacturer of internet-connected televisions, for $2.2 million and fencing-in commitments. Vizio must destroy data and change its practices regarding its tracking of the viewing habits of users of its internet-connected smart TVs and the selling of that data to advertisers without, in the FTC's opinion, adequate consumer notice or choice.

The FTC alleged that Vizio unfairly tracked allegedly sensitive TV-viewing data of millions of American consumers, and deceptively failed to effectively disclose how the collected data was being used. This marks the first time consumer television viewing data has been brought within the FTC's definition of "sensitive" information and emphasizes that companies should provide clear, comprehensive disclosures regarding data collection, use and sharing, especially when such practices may be unexpected. Although the Cable Act, which applies to TV distributors not TV manufacturers, was pointed to as giving TV viewers an expectation of privacy regarding their viewing activities, TV viewing is really no more sensitive than consumer device usage or internet content consumption, thus this action potentially opens a door for a philosophical sea change in the way consumer tracking for interest-based advertising may be treated by regulators in the U.S. Much can be learned from the case.

[31] Lenovo Settles FTC Charges it Harmed Consumers With Preinstalled Software on its Laptops that Compromised Online Security (2017), *available at* https://www.ftc.gov/news-events/press-releases/2017/09/lenovo-settles-ftc-charges-it-harmed-consumers-preinstalled

[32] In the Matter of Lenovo, Complaint, *available at* https://www.ftc.gov/system/files/documents/cases/1523134_lenovo_united_states_complaint.pdf

Complaint

The complaint[33] sets forth a number of allegations regarding Vizio's data collection practices, including:

- In February 2014, Vizio started selling smart TVs loaded with automated content recognition (ACR) software that continuously captured all pixel data from television screens and transmitted that data back to Vizio for comparison and matching using databases of television shows, movies and commercials.
- At the same time, Vizio also remotely installed ACR software on televisions that had originally been sold without it.
- In addition to pixel data about viewing activity, the ACR software collected other information, such as IP addresses, MAC addresses, and Wi-Fi signal strength and local access points, from the connected TVs.
- Vizio then sold the data it collected to third parties for the purposes of measuring audience size, analyzing advertising effectiveness and targeting ads across consumers' devices based on their viewing habits.

The complaint indicates that Vizio's contracts with the third parties to whom it was selling the data prohibited re-identification of individual consumers, but allowed relatively rich data (including sex, age, income, marital status, household size, education, home ownership and household value) to be appended for marketing purposes.

According to the FTC, the televisions that had ACR software preinstalled did not provide any on-screen notice regarding the data collection occurring behind the scenes. TVs that were remotely updated to add ACR software did provide some notice, showing users a pop-up message regarding changes to the Vizio privacy policy (with a URL) and stating that "Smart Interactivity" had been enabled but could be disabled through the settings menu. The FTC claimed that this notice was insufficient, as it did not adequately inform consumers about the comprehensiveness of the data collection or how the data would be shared. Further, although the Smart Interactivity feature was described as providing viewers with program offers and suggestions, the complaint alleges that no such offers or suggestions were actually provided to consumers.

[33] FTC v. Vizio, Inc., Complaint for Permanent Injunction, *available at* https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf

In addition to the monetary payment, going forward Vizio must "prominently disclose" its data collection and sharing practices to consumers, separate from its privacy policy and terms of use (i.e., enhanced notice). The disclosure must list the types of viewing data Vizio will collect and use, the types of viewing data that will be shared with third parties, the identity of those third parties or the categories of the third parties, and the purposes for the sharing. Vizio must then obtain the consumers' affirmative, express consent to the collection and sharing activities and provide instructions on how to revoke such consent.

Vizio also has agreed to destroy, within 120 days of the order, viewing data that it collected prior to March 1, 2016. Similar to other FTC enforcement action settlements discussed above, Vizio will be required to implement a comprehensive privacy program and obtain biennial assessments of its compliance for 20 years.

Takeaways from Vizio

- As suggested by the FTC's Business Center Blog post on the Vizio case,[34] companies that may engage in data collection of this nature should (1) provide clear, user-friendly explanations about their activities up front; (2) obtain consent if they want to collect "highly specific information about [consumers'] entertainment preferences" (preferably affirmative, opt-in consent); and (3) make it easy for people to exercise the choices available to them when it comes to the collection and use of their personal data.
- If opt-outs will be provided, make sure choices are easy for consumers to access and exercise. Descriptions should clearly explain the effects of the opt-out so the consumer knows what opting out will (and will not) accomplish in terms of restricting data collection, use or disclosure.
- The Vizio case may indicate an expansion of the FTC's definition of "sensitive" data that, when collected, used or shared in an unexpected way, may cause the kind of substantial harm that can result in a Section 5 unfairness claim. Such a shift would put television viewing data on par with financial records, health data, Social Security numbers, children's personal information and precise geolocation coordinates in terms of sensitivity. That said, the changing political balance of the commission may reveal this case to be an outlier for the foreseeable future.
- The new majority within the commission may tilt the scales away from interpreting privacy injuries as "substantial," thereby reducing the number of unfairness claims brought in connection with alleged

[34] What Vizio was doing behind the TV screen (2017), *available at* https://www.ftc.gov/news-events/blogs/business-blog/2017/02/what-vizio-was-doing-behind-tv-screen

privacy violations. Nevertheless, failing to provide clear and complete disclosures or omitting material information about data collection and use practices will continue to be viewed as "deceptive" and therefore subject to Section 5 enforcement.

Consumer protection groups advocacy and monitoring

Consumer privacy watchdogs are monitoring IoT data collection and use, and security (or lack thereof) and urging the FTC to take action.

In April 2017, consumer protection group Access Now[35] filed a complaint and request for investigation with the FTC alleging that the $250 internet-connected vibrator manufactured by Svakom and called "Siime Eye," which has a built-in camera and pleasure functions that the user can allow friends to access to view and manipulate sessions, was rife with security vulnerabilities, placing users' privacy at risk. The complaint[36] alleges hackers have proved they can breach security, take over controls and access the camera view, and that while Svakom has promised a "secure connection," the default password is eight 8s, something hackers can easily guess to take over controls and access the camera both via Wi-Fi and the internet.

In October 2017, a coalition of advocacy groups is urging the FTC to look into whether children's smartwatches are posing security and privacy risks.[37] The groups are concerned that potential attackers can take control of apps in the watches and track the location of the watch wearer. Furthermore, the groups are also concerned that children's data are being used for marketing purposes. The Children's Online Privacy Protection Act, and its corresponding regulations, regulate the collection of certain data from children under 13 years of age in connection with websites and mobile applications. This act sets forth tracking disclosure obligations. For more information, see our post here.[38]

---

[35] Access Now asks U.S. FTC to investigate vulnerabilities in internet-enabled sex toy (2017), *available at* https://www.accessnow.org/access-now-asks-u-s-ftc-investigate-vulnerabilities-internet-enabled-sex-toy/
[36] In the matter of Svakom Design USA Limited, *available at* https://www.accessnow.org/cms/assets/uploads/2017/04/AccessNow-FTCComp-Svakom.pdf
[37] FTC Urged To Investigate Smartwatches For Kids (2017), *available at* https://www.mediapost.com/publications/article/308905/ftc-urged-to-investigate-smartwatches-for-kids.html?utm_source=newsletter&utm_medium=email&utm_content=readmore&utm_campaign=105701&hashid=ibWCy22gojGGLBAXlei-Ng-UW7o
[38] Obligations of Online and Mobile Services to Protect Children's Privacy, *available at* https://www.dataprivacymonitor.com/wp-content/uploads/sites/5/2014/09/Alan-Friel-Obligations-of-Online-and-Mobile-Services-Protect-Children-Privacy.pdf

FTC guidance for the IoT industry

The FTC has given the IoT industry specific guidance on what it thinks would constitute reasonable privacy and security protections for IoT devices. This advice, if heeded, would have prevented most of the problems alleged in the cases and incidents discussed above. In June 2016, the FTC staff responded[39] to a Request for Comments from the Commerce Department's National Telecommunications and Information Administration (NTIA), and that followed a January 2015 FTC Staff Report ("Internet of Things: Privacy & Security in a Connected World").[40] From these guidance materials, and the cases and incidents discussed, the following lessons can be discerned:

- Build privacy and security into devices and software at the outset and continuously look for and cure deficiencies.
- Provide a higher level of security for sensitive data.
- Give clear notice of and meaningful choices about data collection, use and sharing to the consumer, particularly if the data is sensitive or its collection, use or sharing would be unexpected.
- Provide info to allow consumers to decide whether and how their data will be collected and used, even for less-than-sensitive data. In some cases this may mean choosing not to buy or use the product, and in others it would mean choosing different options.
- Limit the amount of data collected/retained to what is needed, and limit access to it.
- Secure data and securely dispose of data when no longer needed.
- Train employees on good practices and monitor for knowledge and compliance.
- Ensure downstream privacy and data protections via vendor contracts and oversight.
- Apply defense-in-depth strategies that offer protections at multiple levels and interfaces.
- Employ reasonable access controls.

Potential Legislation

[39] FTC Staff Provides Response to NTIA Request for Comment on Internet of Things (2016), *available at* https://www.ftc.gov/news-events/press-releases/2016/06/ftc-staff-provides-response-ntia-request-comment-internet-things

[40] Internet of Things: Privacy & Security in a Connected World (2015), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

While the FTC guidance is just that, and not law or regulation, it does reflect what the FTC staff thinks is required to avoid a deception or unfairness charge under the FTC's Section 5 authority. It may, however, not be long before there is specific legislation, at least at the state level. CA Senate Bill 327,[41] introduced in February 2017 and amended March 20, 2017, proposes to codify privacy and security by design and allows specific enforcement actions for failure to employ reasonable data protection when developing any device "capable of connecting to the internet, directly or indirectly, or to a connected device," and for failure to promptly patch or otherwise cure later-discovered inadequacies and vulnerabilities. It would also require data collection notices, including a short-form notice at the point of sale regarding audio, video, biometric, health, sensitive or personal info, and require companies to obtain consent before collecting or transmitting such device or consumer information.

Class action lawsuits

The class action plaintiffs' bar is starting to act on the IoT privacy and security vulnerability trend, as evidenced by the March 2017 $3.75 million settlement of a 2016 lawsuit in Illinois regarding the "We-Vibe" marital aid (yes, yet another vibrator case), which allows users to give remote partners the ability to change settings through the internet or mobile connectivity and to live chat during sessions. The plaintiff alleged the manufacturer collected and kept usage info (e.g., times of use, battery life and intensity level) tied to user and partner emails without notice or consent, and that the plaintiff would not have bought the device, which allegedly was more expensive than similar competitor devices, if she had known of the tracking. There were no allegations of security breach or misuse – unjust enrichment, wiretapping and state law privacy violations arising out of the data practices. For more details, see our post here.[42] The latest company to be a target of an IoT privacy class action lawsuit is Bose. The complaint,[43] filed on April 18, 2017, alleges that by using a companion app, the Bose wireless headphones were secretly collecting, transmitting and disclosing customers' private music and audio selections and selling the data to advertisers without notice or consent. On Aug. 3, 2017, Bose filed a motion to dismiss for failure to state a claim, and on Sept. 5, 2017, the plaintiff filed a memorandum in opposition to the motion to dismiss. The lawsuit is still pending.

---

[41] CA Senate Bill 327, *available at* http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327
[42] IoT Device Maker Settles Class Claims for $3.75 Million (2017), *available at* https://www.dataprivacymonitor.com/mobile-privacy/iot-device-maker-settles-class-claims-for-3-75-million/
[43] Kyle Zak v. Bose Corp., *available at* https://www.scribd.com/document/345633440/Zak-v-Bose

The Online Trust Alliance (OTA): IoT Trust Framework

The OTA has released an IoT Trust Framework, which is a product development and risk assessment guide for developers and retailers of IoT devices. The goal of the OTA with this framework is to set forth responsible privacy practices and to bring attention to devices and companies that show a commitment to device security. The framework includes 37 principles and is segmented into the following four categories: (1) security; (2) user access and credentials; (3) privacy, disclosures and transparency; and (4) notifications and related best practices. For more information about the IoT Trust Framework, please see here.[44]

Takeaways

There are lessons to be learned from the cases and incidents to date. First, IoT devices may have the ability to collect all sorts of data, some quite personal or sensitive, and consumers may not expect this data to be collected, used or shared. Next, follow the FTC guidance, including employing privacy-by-design and security-by-design principles. Finally, look to limit your liability with consumers through enforceable consents to clearly stated data and privacy practices, and through limitations on warranties, liability and class actions in user agreements that are affirmatively accepted prior to device data collection. It is also important to understand the challenges[45] and risks unique to IoT devices, and take those into consideration when employing privacy-by design principles and conduction legal compliance reviews.

For more details on IoT privacy and security, and further best practice suggestions, see our posts here[46] and here.[47]

---

[44] IoT Security & Privacy Trust Framework v2.5, *available at* https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf

[45] Challenges include: (1) lack of defined standards; and (2) multi-dimensional risk arising out the combination of apps, platforms, devices, sensors and cloud and web services. Risks include: (1) the consumer role in use of IoT devices (including the need to set and use passwords and security settings); (2) the life of the product and the ongoing need to patch vulnerabilities beyond a typical 90 day to 1 year warranty period; and (3) dependency on third party technologies and platforms.

[46] FTC's $2.2m Smart TV Settlement Signals Continued IoT Enforcement Focus (2017), *available at* https://www.dataprivacymonitor.com/big-data-2/ftcs-2-2m-smart-tv-settlement-signals-continued-iot-enforcement-focus/

[47] Babies and Baby-making, or Not… Privacy and Security Lessons for the Internet of Things (2017), *available at* https://www.dataprivacymonitor.com/internet-of-things/babies-and-baby-making-or-not-privacy-and-security-lessons-for-the-internet-of-things/

Conclusion

In summary, it is best to apply Fair Information Practice (FIP) principles[48] to evolving technology and use privacy by design[49] in the development of cross-device and IoT practices and products to avoid privacy intrusions and security vulnerabilities that could result in regulatory inquiries or class action litigation, or otherwise result in loss of consumer trust or public controversy. Although the law, like the technology, is evolving, it is clear that the FTC expects that companies integrate data privacy and security protections within their businesses at all levels, particularly with regard to consumer data.

[48] Privacy Online: Fair Information Practices in the Electronic Marketplace (2000), *available at* https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf

[49] Protecting Consumer Privacy in an Era of Rapid Change (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf