What We're Reading: Location & Ad Practices

FUTURE OF PRIVACY FORUM

July 2018 Newsletter

Contents:

1. Ad Tech (U.S. & EU)

- The California Consumer Privacy Act (CaCPA), which will become effective on January 1, 2020, grants rights to consumers to request disclosures or deletion of the personal information that a company has collected about that consumer, and also contains provisions for consumers to opt out of information being shared or sold. Here are a few informative resources from the past few weeks:
    - Daniel Solove published a special California Consumer Privacy Act (CCPA) edition of his Privacy + Security newsletter. This edition includes links to a California Consumer Privacy Act Resources page, and links to upcoming workshops on California Privacy Law and the CCPA.
    - OneTrust and IAPP developed a California Consumer Privacy Act Initial Planning Assessment tool to help organizations get a sense of whether they have to comply with CCPA, and, if so, what that might involve. (Martech)
    - The FPF team also developed a comparison of the new California privacy law and the GDPR (available upon request).

- Recent local bills and state laws have implications for Ad Tech, including:
    - Chicago City's proposed Personal Data Collection and Protection Ordinance, which would require businesses to (1) obtain prior opt-in consent from Chicago residents to use, disclose, or sell their personal information, (2) notify affected Chicago residents and the City of Chicago in the event of a data breach, (3) register with the City of Chicago if they qualify as "data brokers," (4) provide specific notification to mobile device users for location services, and (5) obtain prior express consent to use geolocation data from mobile applications.
    - Washington House Bill 2938 (*effective date: June 7, 2018*), which mandates digital communication platforms to provide real-time disclosure of detailed information about election ads in response to public records requests, including

"approximate description of the geographic locations and audiences targeted, and total number of impressions generated by the advertisement or communication."

- The Online Interest-Based Advertising Accountability Program (of the Advertising Self-Regulatory Council/ Council of Better Business Bureaus), which conducts routine monitoring of websites for compliance with the DAA Principles, released two decisions in June that address the issue of **transparency for non-cookie technologies**:
    - One decision (June 7, 2018) finds that x19 Limited, a company based in the United Kingdom that offers a URL shortening service entitled Adf.ly, lacked adequate disclosures for its use of canvas fingerprinting: The Accountability Program found an Adf.ly JavaScript file that appeared to contain code that facilitates canvas fingerprinting on two websites, but it was difficult to determine which terms, if any, from the Adf.ly website governed Adf.ly's collection and use of consumers' browsing data for IBA as a third party. There also appeared to be no available opt-out method.
    - The second decision (June 7, 2018) stated that the company Purple Innovation, LLC, that was previously under inquiry for failure to comply with the enhanced notice requirement of the DAA Principles, is now in full compliance. The company added a link labeled "Interest-based Ads," separate from its "Terms & Privacy" link, on each web page through which third parties collect information for IBA. The link takes users directly to an updated section of the site's privacy policy, which now includes a disclosure of third-party IBA activity occurring on the website, a link to the DAA's page, and a statement of adherence to the DAA Principles.

- Recent & upcoming federal public hearings relevant to Ad Tech:
    - On June 14, 2018, the House Digital Commerce Subcommittee held a hearing to examine the digital advertising ecosystem and its implications for consumer privacy and data protection. Global Chief Privacy Officer of Wunderman Rachel Glasser, one of the expert witnesses, explained how persistent identifiers, like cookies or advertising IDs, track users online without identifying an individual personally, but instead "allows the advertiser to make associations and inferences on types of behavior and the types of things that a consumer enjoys." The Majority Memorandum, witness testimony, and archived webcast are available online here.
    - On June 27-28, 2018, the Federal Election Commission held a hearing on its proposals "to amend its regulations concerning disclaimers on public communications on the internet that contain express advocacy, solicit contributions, or are made by political committees." The FEC agreed in principle that online political ad rules need an update, but commissioners diverged on how such a disclaimer should be formatted and whether the Commission can move fast enough to implement rules before upcoming elections. (The Center for Public Integrity)
    - The FTC announced that the agency will hold a series of public hearings on whether broad-based changes in the economy, evolving business practices, new

technologies, or international developments might require adjustments to competition and consumer protection enforcement law, enforcement priorities, and policy. The hearings will begin in September 2018 and are expected to continue through January 2019, and will consist of 15 to 20 public sessions. (The schedule as it evolves can be found at www.ftc.gov/ftc-hearings). The FTC requests comments on eleven topics, including:

- The intersection between privacy, big data, and competition;
- The Commission's remedial authority to deter unfair and deceptive conduct in privacy and data security matters;
- The consumer welfare implications associated with the use of algorithmic decision tools, artificial intelligence, and predictive analytics;
- The interpretation and harmonization of state and federal statutes and regulations that prohibit unfair and deceptive acts and practices.

- Recent developments in industry approaches and consumer attitudes:
  - A new consumer privacy survey from Acxiom and DMA found that "58% will share personal data under the right circumstances," and that respondents were more aware that their data were being collected than in previous years. (MarTech)
  - Emotion-based targeting has increasingly been a topic of media scrutiny. Reports show publishers like ESPN, The New York Times, and AdExchanger are investing in new technologies to serve users more personalized content based off of their emotional response towards certain topics and stories. (Axios) Ed tech companies are also tracking students feelings "to improve student learning by teaching the software to pinpoint when children are feeling happy, bored, or engaged." (EdWeek)
  - A recent study published in Scientific American found that women see fewer ads related to STEM careers than men because in general women are more expensive to advertise to on social media. Therefore, women are not seeing fewer ads "because of an algorithm responding to click behavior or local prejudice, but instead because women's desirability as a demographic and consequent high price means that an algorithm trained to be cost effective avoids showing ads to them." (Scientific American)
  - Verizon is launched a VPN called Safe Wi-Fi that's being marketed as a way to block targeted advertising, in addition to hiding a user's IP address when they are on a public network. (TechCrunch)

- The Telegraph, Guardian News and Media, and News UK, announced their new platform The Ozone Project - a jointly-owned audience platform - which was developed in response to industry-wide concerns across the digital advertising ecosystem. According the Guardian, the Ozone Project will directly connect brands, agencies, and publishers in an effort to create a more transparent view of how segments are structured and where media is running.

- **European Ad Tech news and developments:**
    - The French data protection authority CNIL published a formal notice (in French) to two location-based mobile advertising companies, Teemo and Fidzup. The CNIL states that these companies are violating the GDPR by collecting certain information (mobile advertising identifier/IDFA, geo-location, and MAC addresses) without appropriate user consent, and without appropriate retention periods. Teemo and Fidzup have been ordered to comply with GDPR within 3 months.
        - CNIL notice (link in French)
        - CNIL's Infographic explaining mobile location data, published the same day (link in French) "Once upon a time – Antoine and the Geolocation of his Smartphone"
        - FPF's informal translations available (on request)
    - The French Competition Authority (FCA) published the results (in French) of its sector-specific inquiry into display online advertising. The sector inquiry pointed out a set of practices considered as potentially detrimental to competition, including (i) strategies involving bundling/tying, "low prices" and exclusivities, (ii) leveraging effects, (iii) discrimination, (iv) restrictions on interoperability and (v) restrictions on the ability to collect and access data. (Kluwer Competition Law Blog)
    - The UK Information Commissioner's Office (ICO) released an interim report on how personal information is used in modern political campaigns. According to the ICO, "one of the most concerning findings from the investigation was a significant shortfall in transparency and provision of fair processing information." The ICO also made ten policy recommendations, including a call for the government to introduce a statutory Code of Practice for the use of personal data in political campaigns.
    - The Council of Europe's Committee of Ministers provided recommendations to member States on guidelines to respect, protect, and fulfill the rights of children in the digital environment. According to the Council, States should put measures in place to address risks like commercial exploitation by "requiring that digital advertising and marketing towards children is clearly distinguishable to them as such, and requiring all relevant stakeholders to limit the processing of children's personal data for commercial purposes."
    - The European Commission published the results of a consumer market study (July 19) on "online market segmentation through personalised pricing/offers in the European Union," finding evidence of personalized ranking, i.e. websites changing the order of search results when different consumers search for the same products online, based on information about the shoppers' access route to the website or based on information about the shoppers' past online behavior). The study did *not* find evidence of "consistent and systematic personalised pricing."

2. Location Data:

- Supreme Court ruled that warrants are required for law enforcement to collect cell-site location information (CSLI data) from mobile carriers. According to the majority, "Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts....These location records "hold for many Americans the 'privacies of life.'" Riley, 573 U. S. 400 (slip op., at 28) (quoting Boyd, 116 U. S., at 630). The Court rejected the government's argument that there was no 4th Amendment protection in this data because it was previously disclosed to a third party, given the unique nature and persistence of cell phone location records. Potential implications of the Carpenter decision range from establishing a basis for private companies to push back against government requests for CSLI data, to providing support for extending privacy protections to other forms of location data as well.
    - Blog posts by ZwillGen and Ropes & Gray provide excellent summaries and analysis of the *Carpenter* decision.
    - Listen to IAPP's Privacy Advisor Podcast (July 27) for a discussion with Professor Orin Kerr of the USC Gould School of Law and Jennifer Granick of the American Civil Liberties Union discussing why the case is so significant and what it could mean for the future of law enforcement access to location data.

- The ACLU of Northern California analyzed the data collection practices of three top bikeshare/scooter companies, calling for clearer privacy policies, data minimization, and strong security programs (July 25). (Fast Company)

- In late June, major wireless carriers announced they would stop the sale of customers' location data to certain third parties in response to an investigation into the common practice by Sen. Ron Wyden. (Associated Press) (*See Sen Wyden's letter to the FCC, asking the Commission to investigate, and initial response letters from Verizon, T-Mobile, Sprint, and AT&T.*) Before those announcements were made, web archives indicate that a bail bond company called Captira was purchasing cell phone geolocation location data from wireless carriers and selling it to bounty hunters. Captira advertised that it would "instantly locate defendant cell phone" for as little as $7.50. (Motherboard)

- Spain's La Liga soccer league used its official app to detect the GPS location of Android users, and if they were found to be in a sports bar, the app then accessed users' microphones and recorded audio data to detect illegal broadcasting. In a statement on its website (in Spanish), La Liga explained that it was attempting to locate venues illegally broadcasting games, and requested app users' permission to access their microphones. The Spanish Agency for Data Protection (AEPD) has now opened a preliminary investigation into the activity. (BBC, Fast Company, El Diario).

- In a recent study, researchers reviewed the problems faced by institutional review boards reviewing the use of mobile location data in biomedical research, and suggested 6 questions that these boards should be asking, including "What are the risks of collecting, sharing, and publishing individual-level location-based data?" The authors

also outline a number of technical mitigation strategies, some of which require a data scientist. (Endocrinology Advisor)

- The Open Data Institute (ODI) is launching a series of new projects, including one which will explore ways to support and enable the publication and use of open geo-spatial data. In order to accomplish this goal, the ODI has developed a data ecosystem mapping tool in order to create visual map that illustrates how data is being accessed, used, and shared by a variety of organizations, from Pokemon Go to flood data. (Open Data Institute)

3. Platforms and Apps:

- Northeastern University computer science academics conducted a rigorous study that debunked the myth that smartphones are secretly listening to users. However, the researchers found that screenshots and video recordings of what people were doing in apps were being sent to third parties, potentially in violation of their own privacy policies (when the practice is not disclosed) and app store policies. (Gizmodo)

- Privacy advocates wrote a letter to the FTC, urging the Commission to investigate "the misleading and manipulative tactics of the dominant digital platforms in the United States, which steer users to 'consent' to privacy-invasive default settings," after the Norwegian Consumer Council released a report examining the default privacy settings of Facebook, Google and Windows 10. (IAPP)

- Highlighting recent reports on the trend of single-use apps becoming social networks, and the privacy concerns that come with this trend: Venmo, for example, has recently received attention for its "public by default" transaction settings, which makes it possible for view a Venmo user's purchase history. (Wired, ZDnet) Venmo supports the default public setting of its app: *"We make it default because it's fun to share [information] with friends in the social world." "[We've seen that] people open up Venmo to see what their family and friends are up to."* (CNET)

- Five digital advertising trade associations wrote an open letter in response to Apple's WWDC announcements of upcoming privacy features in Safari, expressing concerns over the economic model of personalized advertising. For example, the groups said that limiting browser fingerprinting "will not only hurt advertisers' ability to reach the right consumers, but also limit the effectiveness of security systems and anti-fraud tools that use such identifiers."

4. Smart Homes and the "Internet of Things":

- Consumer Product Safety Commission (CPSC)'s Request for Comments on potential safety issues and hazards associated with Internet-connected consumer product closed on June 15, 2018. The FTC's Bureau of Consumer Protection (BCP) response was among relevant comments. While the CPSC noted that privacy and data security are outside the scope of its inquiry, the BCP emphasized that poor security in IoT devices might create technology-related hazards associated with the loss of critical safety function, loss of connectivity, or degradation of data integrity. For example, a car's braking system might fail if infected with malware, or carbon monoxide or fire detectors could stop working if they lose their Internet connection. (FTC Press Release)

- On July 19, 2018, NTIA convened a multistakeholder process to develop greater transparency of software components for better security across the digital ecosystem. (NTIA Blog) In particular, a software "bill of materials" (SBoM) - a centralized comprehensive list of components contained within a product - was considered as a tool in advancing IoT software component transparency. (*Note: The FDA recently announced plans to require firms to develop an SBoM that must be provided to the FDA and made available to medical device customers and users*). While standardizing the adoption of SBoMs may be beneficial in many ways (e.g., helping customers to make informed security decisions), SBoMs may be a controversial idea because of the diversity of consumers involved and the implications for intellectual property, software liability, and insurance. The next NTIA multistakeholder meeting on this topic will be a virtual meeting in September 2018. (NTIA)

- *The New York Times* reported on how connected home devices have increasingly been used in domestic abuse cases over the past year. Internet-connected locks, speakers, thermostats, lights and cameras that have been marketed as the newest conveniences are now also being used as a means for harassment, monitoring, revenge and control. The Safety Net Project at the National Network to End Domestic Violence (NNEDV) recently published a guide to assist in better understanding of IoT in domestic violence cases.

- In early July, The New York Times reported on TV viewer tracking and personalized ads, explaining that consumers may not know how much information a television company is collecting to send personalized ads or make show recommendations. For example, Samba TV can analyze what viewers are watching, determine how many connected devices viewers have in the house, and then target them with ads. (See Samba's press release on its compliance with GDPR here) Last week, The New York Times published a follow-up article that explains how users can disable tracking on various kinds of Smart TVs.

Did we miss anything? Send us your thoughts at cmarlowe@fpf.org or sgray@fpf.org.