Hands in the Cookie Jar: Internet Cookie Consent in the Online Advertising Industry

A Sociotechnical Research Paper
presented to the faculty of the
School of Engineering and Applied Science
University of Virginia

by

Jack Schefer

May 7, 2021

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Jack Schefer

Sociotechnical advisor: Peter Norton, Department of Engineering and Society

Hands in the Cookie Jar: Internet Cookie Consent in the Online Advertising Industry

Facebook earned over $70.6 billion in revenue in 2019, yet their major platforms, such as Facebook, Instagram, Facebook Messenger, and WhatsApp, remain nominally free to users. Over 98.5% of their revenue came from advertising (Facebook, Inc., 2020a). Targeted advertising, or the careful tracking of user behavior to inform which advertisements get served to which users, relies on an immense network of data collection. The most common mechanism for tracking user behavior across multiple sites is the internet cookie (Miyazaki, 2008). Cookies allow websites to store information on user devices which can be retrieved by the same website on any future access. Advertisers leverage this technology to identify and track users every time an advertisement appears on-screen across any of the sites in their network.

As governments regulate online privacy and data collection practices, users and corporations compete for sway. While consumers seek privacy and autonomy online, corporations fight to maximize the size and monetizability of their user bases with minimal interference. Government regulation of Internet cookies is a case study in this broader struggle and consent for cookie use is a key subject of debate. Understanding how the struggle unfolds is critical to analyzing current government action and whether it is sufficient to protect consumer rights. In the United States, the regulatory environment surrounding cookie consent fails to ensure consent to data collection is valid, informed, and affirmative. This is an immensely dangerous precedent as new behavioral tracking technologies continue to emerge.

Review of Research

Definitions of consent have been studied by philosophers like Kant, Locke, and Socrates. Konow presents an overview of what constitutes consent across disciplines and contrasts this

with coercion (2014). Den Hartogh further analyzes whether consent can be presumed, focusing primarily on the medical field (2011). Susser examines Internet cookie notices specifically and argues that while mere notices do not promote legitimate consent, they can still be beneficial and inform users (2019). McStay surveys historical and practical factors underlying the European Union's modern notion of cookie consent as evidenced in documents like the ePrivacy directive and the cookie directive (2012). Both Susser and McStay differentiate the passive cookie notices from the more active choice mechanisms in their research.

Research also examines the user perspective of cookie consent. Psychological factors like risk perception, power perception, and consumer trust are prominent areas of study (Bornshein et al., 2020; Chen & Atkin, 2020; Miyazaki, 2008; Miyazaki & Krishnamurthy, 2002). Further research focuses on user understanding of cookie technology (Jensen et al., 2005; Pierson & Heyman, 2011).

Corporate action and response to regulation has also been a focus of study. Bornschein et al. find that compliance with the EU's General Data Protection Regulation (GDPR) varies significantly between companies. De & Imine present a detailed analysis of Facebook's privacy policy specifically and find it non-compliant on multiple counts related to consent (2020).

Legal experts have worked to summarize current regulatory enforcement in the US and its legal consequences (McSweeny, 2017; Solove & Hartzog, 2014). Others have critically analyzed individual cases and enforcement actions (Black & Steel, 2016; Khan, 2011). More robust analyses of European privacy law exist though these offer limited applicability to the US system (Bornshein et al., 2020; Breen et al., 2020).

This work summarizes consumer and corporate actions in the competition for regulatory influence and then evaluates the resulting environment, all with focus on Internet cookie consent.

User Disinterest

Most Internet users lack a technical understanding of cookies, undermining any mechanism for informed consent. While 90.3% of users claim knowledge of cookies for online tracking, only 14% can demonstrate a basic understanding when probed (Jensen et al., 2005; Miyazaki, 2008). Initial proposals for the standardization of cookie technology, however, relied on an active and informed user to monitor their own privacy. In response to privacy concerns, designers specified that users must be able to view and delete cookies in their web browser which relies on technical aptitude (Kristol & Montulli, 1997). Scholars point out that expecting rigorous technical knowledge from every user is unrealistic, but there are parallels in political thought and medicine where consent can be given under "adequate apprehension" of risks (McStay, 2012). Finally, Pierson and Heyman conclude that lack of technical knowledge prevents an accurate assessment of risks and benefits during evaluation of cookie usage, invalidating any provided consent (2011).

Psychological factors also affect online users. Consumers are generally wary of the behavioral tracking and data mining practices that cookies enable. As the surveys of Kennedy et al. summarize, user attitudes on fairness stem from "a discrepancy between the practices of the platforms and users' normative expectations" (2017). Pierson and Heyman come to a similar conclusion, arguing that a lack of "contextual integrity" is the cause of tracking aversion. Thus, breaches of privacy and fairness come from using freely given information for purposes outside of the user's intent (Pierson & Heyman, 2011). The mechanism by which cookie notification is presented to users has been shown to affect psychological privacy perceptions. Bornschein et al. demonstrate that mere notification of cookie use increases perceived risk whereas offering a choice during notification reduces risk perception through user empowerment. These perceptions

then have an observable effect on usage and purchasing decisions (Bornschein et al., 2020; Miyazaki, 2008).

Consumer advocacy groups have also been active on broader Internet privacy issues. When Facebook CEO Mark Zuckerberg testified before Congress in the wake of the Cambridge Analytica scandal, the American Civil Liberties Union (ACLU) raised concerns of data ownership and urged congress to "enact [the] comprehensive privacy legislation" that the US needs (ACLU, 2018). The Electronic Privacy Information Center (EPIC) more specifically targets Internet privacy issues such as non-consensual cookie use. Founded in 1994, EPIC conducts policy research and files amicus curiae briefs in relevant legal cases (EPIC, n.d.). The Center for Digital Democracy (CDD) submits reports to the Federal Trade Commission (FTC) for investigation but warns that "we need a new digital watchdog" to augment FTC enforcement (Chester, 2019). In a joint report with the US Public Interest Research Group (USPIRG), the CDD advocated for consumer ownership of data and comprehensive federal regulations on data privacy as early as 2009. The joint report also notes the need for user education to drive informed consent, privacy concerns with cookie use specifically, and the dangers of opt-out consent mechanisms (CDD & U.S. PIRG, 2009).

Corporate Self-Interest

Large technology companies in the behavioral advertising industry have a stake in any discussion affecting the data they can track and the methods they can use to operate. Behavioral data has become the "primary commodity on the web for brokers and advertisers" (Frow, 2019) and a cornerstone of the business model responsible for 98.5% and 85.4% of revenue at Facebook and Alphabet, respectively, in 2018 (Facebook Inc., 2020a; Alphabet Inc., 2020). Competition in the advertising industry incentivizes data collectors to continually increase

targeting capabilities, though Kox et al. theorize that allowing users to self-select privacy preferences would increase overall economic welfare (2018).

Critics of corporate respect for privacy argue that business actions are self-serving. These critics start their examination with privacy policies. McStay argues that privacy policies protect corporations rather than their customers (McStay, 2012). Fernback and Papacharissi go further in their criticism, calling privacy policies "evidence of the internet industry's self-protective efforts at the expense of consumer privacy." Their research concludes that privacy policies are too dense for the average English speaker to understand and that risks are "lost in the obfuscatory language, unclear or undefined policies" of the statements (Fernback & Papacharissi, 2007). Facebook's policy, particularly their policy on cookies, serves as an example (Facebook Inc., 2020b). Aspects of the policy are quite transparent; the examples are illustrative and detail is taken to the meaning of each individual cookie name. However, individual cookie names and the significance of their lifespan is likely inaccessible language to the average consumer. Accusations of corporate self-interest also stem from conflicting public statements. In 2019, Facebook CEO Mark Zuckerberg released a statement deflecting privacy responsibility to the government urging a need for regulation to "establish a way to hold companies such as Facebook accountable by imposing sanctions when we make mistakes" (Zuckerberg, 2019). This is in juxtaposition to previous statements arguing that Facebook "not only [wants] to comply with the law, but also go beyond [their] obligations" (Facebook Inc., 2018).

Corporate attempts at self-regulation are also self-serving. The Digital Advertising Alliance (DAA) publishes and maintains guidelines for ethical practices but has limited enforcement. Its website currently lists 266 corporate members, including prominent social media companies, advertising networks, and consumer goods manufacturers (Digital Advertising

Alliance, n.d.). The DAA defines consent as "an individual's action in response to a clear, meaningful and prominent notice regarding collection and use of data" and specifies that changes to policy invalidate previous consent agreements. When the DAA finds a violation, a written report is published but more serious sanctions must be carried out by government watchdogs (Digital Advertising Alliance, 2009). The TRUSTe certification program is another accountability mechanism where companies can voluntarily submit to compliance checking for things like cookie consent and advertisement selection (TrustArc Inc., n.d.). However, both of these self-regulatory organizations ultimately rely on government action. Additionally, researchers conclude that participation in self-regulatory programs does not affect privacy implementation outcomes but does improve consumer perception (Miyazaki & Krishnamurthy, 2002; Listokin, 2015).

Academics also suggest parallels between the practices of behavioral advertising companies and the methods of psychological research. Crucial to both social media and advertising companies are the algorithms used to determine what users see and when. Thus, to stay competitive these companies must continually improve their algorithms to present users with better or more applicable content. Experimentation occurs continually by changing the algorithm incrementally, observing user behavior, then repeating. In 2012, Facebook went a step further and ran an experiment by actively manipulating the order of News Feed content and measuring the observable emotional response (Kramer et al., 2014). After publishing their findings, backlash ensued both in the academic community as well in popular news (BBC News, 2014; Goel, 2014). Facebook argued that by agreeing to the data policy at the time, users consented to having their data used for such purposes. Critics pointed out that the policy did not

mention research or content manipulation, knowledge of which would predicate informed consent in behavioral psychology (Shaw, 2016; McStay, 2012).

Finally, large companies promote lenient legislation through political spending. Large technology companies spend millions of dollars on government lobbying every year. With the exception of Google, the trend in recent years has been a steady increase (Feiner, 2020; Feiner, 2021). The Washington Post estimates that "just seven tech giants [accounted] for nearly half a billion dollars in lobbying over the past decade" (Romm, 2020). However, such aggregate spending numbers reflect lobbying on an entire policy agenda and are not specific to privacy regulation. Reporters at Bloomberg Law add that "spending to support highly influential think tanks and public interest groups" allow companies to "shape the privacy debate, ostensibly as independent observers." Data on this type of spending is more difficult to find. Jeff Chester, the director of the aforementioned CDD which does not accept such donations, worries that think-tank funding allows corporations to exert a strong, undocumented influence (Stoller, 2019).

Unhurried Government Action

The regulatory environment surrounding cookie consent is complex. The United States lacks comprehensive internet privacy laws and has historically used the FTC to monitor corporate action (Government Accountability Office, 2019).

Niche Regulation

The US lacks comprehensive data privacy legislation at the federal level but individual states, most notably California, have enacted laws establishing digital privacy rights for their residents. The California Consumer Privacy Act of 2018 (CCPA) is the most well-known of such statutes and establishes a person's right to know what personal information gets collected about

them and the right to delete such data. Regarding consent, the code asserts that businesses collecting personal data must, "at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used" (California Consumer Privacy Act of 2018, 2018). The CCPA's requirement of merely informing users allows passive notices to be compliant. The CCPA requires active, affirmative consent only when selling personal information to third parties, not for the collection itself or internal uses (Office of the Attorney General, n.d.). According to the International Association of Privacy Professionals, only Virginia has passed a comparably comprehensive privacy law though many other states are in the process of doing so (Rippy, 2021).

The Children's Online Privacy Protection Act (COPPA) is a federal law aiming to protect children under the age of 13 on the Internet. As such, the act mandates that sites must "obtain verifiable parental consent before any collection, use, or disclosure of personal information from children" (Children's Online Privacy Protection Rule, 2021). The language of COPPA requires parental consent to be active and lists acceptable methods. However, the FTC acknowledges that "current technology does not provide a practical means to prevent determined children from falsifying their age online" (FTC, 2007). The potential to falsify age online with ease prevents COPPA from truly requiring parental consent. Like the CCPA, the COPPA only applies to a small portion of the general US population and even within this niche it fails to require adequate consent mechanisms.

Variable Case Enforcement

The FTC maintains jurisdiction over potentially unfair business practices but cannot effectively do so. According to the Government Accountability Office (GAO), between 2008 and

2018 the FTC acted on 101 cases relating to Internet privacy. Cases alleged various harms, ranging from unfair and deceptive corporate practices to COPPA violations. Few such cases were actually litigated. The GAO also warns that the commission's inability to levy civil penalties for first offenses under section 5 of the FTC Act hamstrings its enforcement capabilities (2019). FTC Commissioner, and now chair, Rebecca Slaughter testified before Congress in 2018 that "no matter how big the breach or how egregious the conduct, the FTC has no authority to seek financial penalties for most types of abuse or misuse of consumer data." Slaughter also urged legislators to increase FTC funding or risk an inability to litigate cases against wealthy corporations (*Federal Trade Commission Oversight*, 2018).

In 2012, the FTC issued a complaint against Facebook alleging deceptive data privacy practices, illuminating it's working definition of consent. In the second of eight counts against Facebook, the FTC alleged that "Facebook failed to disclose, or failed to disclose adequately, that, following the December Privacy Changes, users could no longer restrict access to their Name, Profile Picture, Gender, Friend List, Pages, or Networks by using privacy settings previously available to them." Classifying this failure of disclosure as a deceptive act or practice affirms the importance of being informed in the FTC's ideal of consent. The following count states:

> By designating certain user profile information publicly available that previously had been subject to privacy settings, *Facebook materially changed its promises* [emphasis added] that users could keep such information private. Facebook retroactively applied these changes to personal information that it had previously collected from users, without their informed consent... This practice constitutes an unfair act or practice. (*Federal Trade Commission v. Facebook, Inc.*, 2012)

Thus, according to the FTC not only must digital consent be informed, it also must be reaffirmed if the circumstances under which consent was given change. The FTC could not legally fine Facebook for the initial offense. In 2019, 7 years after filing the initial order, the FTC issued penalties against Facebook for failure to comply. The $5 billion penalty, accompanied by additional operational restrictions, was "almost 20 times greater than the largest privacy or data security penalty ever imposed worldwide" (FTC, 2019). Note that $5 billion represents just over 7% of Facebook's gross revenue and 27% of its net income that year (Facebook Inc., 2020a)

The FTC's 2017 case against Vizio, alleging improper and deceptive tracking of Internet-enabled televisions, further expands the FTC's definition of digital consent. The filing asserts that Vizio tracked users without consent but emphasizes that the tracking occurred "through a medium that consumers would not expect" raising the possibility that consent could have been implied if the collection vector was more obvious (*Federal Trade Commission v. Vizio, Inc.*, 2017). Press releases covering the $2.2 million sanctions state that Vizio must "prominently disclose and obtain affirmative express consent for its data collection and sharing practices" going forward (FTC, 2017). Note that the $2.2 million penalty represents just 1.2% of Vizio's revenue and 9.5% of Vizio's net income in 2019 (Vizio Holding Corp., 2021).

Legal scholars disagree on the efficacy of the current regulatory environment. Solove & Hartzog note that FTC cases "have nearly all resulted in settlement agreements" but argue that "companies look to these agreements to guide their privacy practices" effectively building a body of precedent that is functionally equivalent to common law statutes (2014). After analyzing FTC case enforcement, McSweeny concludes that "the FTC has taken the view that consent... may be inferred based on consumers' reasonable expectations consistent with the context of a particular

transaction" (2017). McSweeny critiques the case enforcement system noting that a body of precedent fails to provide sufficiently clear privacy guidance due to its *ex post* nature.

Conclusion

The behavioral advertising industry funds the Internet of today but poses significant dangers to user privacy and autonomy. A lack of general consumer knowledge surrounding cookie technology and a lack of transparency from corporate actors obstruct users from giving truly informed consent. Further, users and regulators are appeased by self-serving corporate statements and self-regulatory groups that lack weight, substantiation, and enforcement capabilities. Corporations use their wealth to lobby, fund policy research, and litigate cases that users and the FTC cannot keep up with. The FTC's stance on consent to data collection practices, when it even has the power to affect change, is that continued use implies consent unless the collection method is unexpected, deceptive, or predatory. This is inconsistent with definitions of affirmative consent in other domains.

The path to an improved future is unclear. Cookie notices should not go away because, as academics point out, at a minimum they promote awareness of data collection practices. Continued user education is vital so that costs and benefits can be adequately weighed before consent is given. Congressional action on digital rights is needed. Rather than hindering innovation, a unified federal code would reduce the complexity of overlapping state laws and further empower the FTC to protect consumer rights. The FTC either needs an increase in resources and authority, or to be augmented with a new consumer protection agency. Rolling out such changes is not easy, but legislators can learn from the European Union's progress and stumbles. Until users are empowered and laissez-faire privacy enforcement ends, user exploitation will continue to prevail.

References

Alphabet Inc. (2020). *Alphabet Annual Report 2019*. Alphabet Inc. https://abc.xyz/investor/static/pdf/2019_alphabet_annual_report.pdf?cache=c3a4858

American Civil Liberties Union. (2018, April 10). *ACLU Comment on Mark Zuckerberg Senate Testimony*. American Civil Liberties Union. https://www.aclu.org/press-releases/aclu-comment-mark-zuckerberg-senate-testimony

BBC News. (2014, June 30). *Facebook emotion experiment sparks criticism*. https://www.bbc.com/news/technology-28051930

Black, J., & Steel, J. (2016). Privacy Developments: Private Litigation, Enforcement Actions, Legislation, and Administrative Actions. *The Business Lawyer*, *72*(1), 207–220. https://www.jstor.org/stable/10.2307/26419117

Bornshein, R., Schidt, L., & Maier, E. (2020). The Effect of Consumers' Perceived Power and Risk in Digital Information Privacy: The Example of Cookie Notices. *American Marketing Association*, *39*(2), 135–154. https://doi.org/10.1177/0743915620902143

Breen, S., Ouazzane, K., & Patel, P. (2020). GDPR: Is your consent valid? *Business Information Review*, *37*(1), 19–24. https://doi.org/10.1177/0266382120903254

California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100-1798.199.100 (2018). https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

Center for Digital Democracy, & U.S. Public Interest Research Group. (2009). *CDD and USPIRG File Comments with FTC on Privacy and Behavioral Targeting*. Center for Digital Democracy. https://www.democraticmedia.org/cdd-uspirg

Chen, H., & Atkin, D. (2020). Understanding third-person perception about Internet privacy risks. *New Media & Society*, 1–19. https://doi.org/10.1177/1461444820902103

Chester, J. (2019). *FTC Facebook decision must go beyond Cambridge Analytica--that's just was the tipping point*. Center for Digital Democracy. https://www.democraticmedia.org/article/ftc-facebook-decision-must-go-beyond-cambridge-analytica-thats-just-was-tipping-point

Children's Online Privacy Protection Rule, 16 CFR §312.5 (2021). https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5#se16.1.312_15

De, S. J., & Imine, A. (2020). Consent for targeted advertising: the case of Facebook. *AI & Society*, *35*, 1055–1064. https://doi.org/10.1007/s00146-020-00981-5

Den Hartogh, G. (2011). Can Consent be Presumed? *Journal of Applied Philosophy*, *28*(3), 295–307. https://doi.org/10.1111/j.1468-5930.2011.00524.x

Digital Advertising Alliance. (n.d.). *DAA Participating Companies & Organizations*. https://digitaladvertisingalliance.org/participating

Digital Advertising Alliance. (2009). *Self-Regulatory Principles for Online Behavioral Advertising*. Digital Advertising Alliance. https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/seven-principles-07-01-09.pdf

Electronic Privacy Information Center. (n.d.). *About EPIC*. Electronic Privacy Information Center. https://epic.org/epic/about.html

Facebook Inc. (2018). *Complying With New Privacy Laws and Offering New Privacy Protections to Everyone, No Matter Where You Live*. Facebook Inc. https://about.fb.com/news/2018/04/new-privacy-protections/

Facebook Inc. (2020a). *Facebook Annual Report 2019*. Facebook Inc. http://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/45290cc0-656d-4a88-a2f3-147c8de86506.pdf

Facebook Inc. (2020b, October 5). *Cookies & other storage technologies*. Facebook. https://www.facebook.com/policies/cookies/

Federal Trade Commission. (2007). *Implementing the Children's Online Privacy Protection Act*. https://www.ftc.gov/sites/default/files/documents/reports/implementing-childrens-online-privacy-protection-act-federal-trade-commission-report-congress/07coppa_report_to_congress.pdf

Federal Trade Commission. (2017). *VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent*. https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it

Federal Trade Commission. (2019, July 24). *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*. https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

Federal Trade Commission v. Facebook, Inc., C–4365 (2012). https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf

Federal Trade Commission v. Vizio, Inc., 2:17-cv–00758 (United States District Court, District of New Jersey 2017). https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf

Feiner, L. (2020, January 22). Google cut its lobbying spending nearly in half in 2019, while Facebook took the lead. *CNBC*.

https://www.cnbc.com/2020/01/22/how-much-google-facebook-amazon-and-apple-spent-on-lobbying-in-2019.html

Feiner, L. (2021, January 22). Facebook spent more on lobbying than any other Big Tech company in 2020. *CNBC*. https://www.cnbc.com/2021/01/22/facebook-spent-more-on-lobbying-than-any-other-big-tech-company-in-2020.html

Fernback, J., & Papcharissi, Z. (2007). Online privacy as legal safeguard: the relationship among consumer, online portal, and privacy policy. *New Media & Society*, *9*(5), 715–734. https://doi.org/10.1177/1461444807080336

Frow, J. (2019). Cookie. *Cultural Studies Review*, *25*(2), 208–210. https://doi.org/10.5130/csr.v25i2.6899

Goel, V. (2014, June 29). Facebook Tinkers With Users' Emotions in News Feed Experiment, Stirring Outcry. *The New York Times*. https://www.nytimes.com/2014/06/30/technology/facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirring-outcry.html

Government Accountability Office. (2019). *Internet Privacy: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility* (GAO-19-52). https://www.gao.gov/assets/gao-19-52.pdf

Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of Internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies*, *63*(1–2), 203–227. https://doi.org/10.1016/j.ijhcs.2005.04.019

Kennedy, H., Elgesem, D., & Miguel, C. (2017). On fairness: User perspectives on social media data mining. *Convergence: The International Journal of Research into New Media Technologies*, *23*(3), 270–288. https://doi.org/10.1177/1354856515592507

Khan, F. (2011). Survey of Recent FTC Privacy Developments and Enforcement. *The Business Lawyer*, *67*(1), 297–303. http://www.jstor.com/stable/41348302

Konow, J. (2014). Coercion and Consent. *Journal of Institutional and Theoretical Economics*, *170*(1), 49–74. https://doi.org/10.1628/093245614X13871984731086

Kox, H., Straathof, B., & Zwart, G. (2018). Targeted advertising, platform competition, and privacy. *Journal of Economics & Management Strategy*, *26*(3), 557–570. https://doi.org/10.1111/jems.12200

Kramer, A., Guillory, J., & Hancock, J. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences*, *111*(24), 8788–8790. https://doi.org/10.1073/pnas.1320040111

Kristol, D., & Montulli, L. (1997). *RFC 2109: HTTP State Management Mechanism*. IEEE Network Working Group. https://www.ietf.org/rfc/rfc2109.txt

Listokin, S. (2015). Industry Self-Regulation of Consumer Data Privacy and Security. *The John Marshall Journal of Information Technology & Privacy Law*, *32*(1).

McStay, A. (2012). I consent: An analysis of the Cookie Directive and its implications for UK behavioral advertising. *New Media & Society*, *15*(4), 596–611. https://doi.org/10.1177/1461444812458434

McSweeny, T. (2017). FTC 2.0: Keeping Pace with Online Platforms. *Berkeley Technology Law Journal*, *32*(3), 1027–1050. https://doi.org/10.2307/26488976

Miyazaki, A. (2008). Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage. *Journal of Public Policy & Marketing*, *27*(1), 19–33. https://doi.org/10.1509/jppm.27.1.19

Miyazaki, A., & Krishnamurthy, S. (2002). Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions. *The Journal of Consumer Affairs*, *36*(1), 28–49. https://doi.org/10.2307/23860158

Office of the Attorney General. (n.d.). *California Consumer Privacy Act (CCPA)*. https://oag.ca.gov/privacy/ccpa

Pierson, J., & Heyman, R. (2011). Social media and cookies: challenges for online privacy. *Info : The Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media*, *13*(6), 30–42. https://doi.org/10.1108/14636691111174243

Rippy, S. (2021, March 22). *US State Comprehensive Privacy Law*. International Association of Privacy Professionals. https://iapp.org/resources/article/state-comparison-table/

Romm, T. (2020, January 22). Tech giants led by Amazon, Facebook and Google spent nearly half a billion on lobbying over the past decade, new data shows. *The Washington Post*. https://www.washingtonpost.com/technology/2020/01/22/amazon-facebook-google-lobbying-2019/

Shaw, D. (2016). Facebook's flawed emotion experiment: Antisocial research on social network users. *Research Ethics*, *12*(1), 29–34. https://doi.org/10.1177/1747016115579535

Federal Trade Commission Oversight: Hearing before the U.S. Senate Commerce, Science,and Transportation Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security, 115th Cong. (2018) (testimony of Rebecca Slaughter), https://www.c-span.org/video/?455021-1/federal-trade-commission-oversight

Solove, D., & Hartzog, W. (2014). The FTC and the New Common Law of Privacy. *Columbia Law Review*, *114*(3), 583–676. https://www.jstor.org/stable/23723427

Stoller, D. (2019, November 18). Facebook, Google Fund Groups Shaping Federal Privacy Debate (3). *Bloomberg Law*. https://news.bloomberglaw.com/tech-and-telecom-law/facebook-google-donate-heavily-to-privacy-advocacy-groups

Susser, D. (2019). Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't. *Journal of Information Policy*, *9*, 37–62. https://doi.org/10.5325/jinfopoli.9.2019.0037

TrustArc Inc. (n.d.). *TrustArc*. https://trustarc.com

Vizio Holding Corp. (2021). *Form S-1 Registration Statement*. https://www.sec.gov/Archives/edgar/data/1835591/000119312521062802/d87723ds1.htm

Zuckerberg, M. (2019). *Four Ideas to Regulate the Internet*. Facebook Inc. https://about.fb.com/news/2019/03/four-ideas-regulate-internet/