Tracking on the Web, Mobile and the Internet of Things

Other titles in Foundations and Trends® in Web Science

An Introduction to Hybrid Human-Machine Information Systems
Gianluca Demartini, Djellel Eddine Difallah, Ujwal Gadiraju and Michele Catasta
ISBN: 978-1-68083-374-4

Minds Online: The Interface between Web Science, Cognitive Science and the Philosophy of Mind
Paul Smart, Robert Clowes and Richard Heersmink
ISBN: 978-1-68083-322-5

Collective Attention on the Web
Christian Bauckhage and Kristian Kersting
ISBN: 978-1-68083-204-4

Tracking on the Web, Mobile and the Internet of Things

Reuben Binns
University of Oxford
UK
reuben.binns@cs.ox.ac.uk

now
the essence of knowledge
Boston — Delft

Foundations and Trends® in Web Science

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

R. Binns. *Tracking on the Web, Mobile and the Internet of Things*. Foundations and Trends® in Web Science, vol. 8, no. 1–2, pp. 1–113, 2022.

ISBN: 978-1-68083-965-4

Foundations and Trends® in Web Science
Volume 8, Issue 1–2, 2022

Editorial Board

Editorial Scope

Topics

Foundations and Trends® in Web Science publishes survey and tutorial articles in the following topics:

- Agents and the Semantic Web
- Collective Intelligence
- Content Management
- Databases on the Web
- Data Mining
- Democracy and the Web
- Dependability
- Economics of information and the Web
- E-Crime
- E-Government
- Emergent behaviour
- Ethics
- Hypertext/Hypermedia
- Identity
- Languages on the Web
- Memories for Life
- Mobile/Pervasive
- Network Infrastructures
- Performance
- Privacy
- Scalability
- Security
- Semantic Web
- Social Networking
- Standards
- The Law and the Web
- The Web as an Educational Tool
- The Web in the Developing World
- Trust and Provenance
- Universal Usability
- User Interfaces
- Virtual Reality
- Web Art
- Web Governance
- Search
- Web Services

Information for Librarians

Foundations and Trends® in Web Science, 2022, Volume 8, 4 issues. ISSN paper version 1551-3939. ISSN online version 1551-3947. Also available as a combined paper and online subscription.

Contents

Tracking on the Web, Mobile and the Internet of Things

Reuben Binns

University of Oxford, UK; reuben.binns@cs.ox.ac.uk

ABSTRACT

"Tracking" is the collection of data about an individual's activity across multiple distinct contexts and the retention, use, or sharing of data derived from that activity outside the context in which it occurred. This monograph aims to introduce tracking on the web, smartphones, and the Internet of Things to an audience with little or no previous knowledge. It covers these topics primarily from the perspective of computer science and human–computer interaction, but also includes relevant law and policy aspects. Rather than a systematic literature review, it aims to provide an overarching narrative spanning this large research space.

Section 1 introduces the concept of tracking. Section 2 provides a short history of the major developments of tracking on the web. Section 3 presents research covering the detection, measurement and analysis of web tracking technologies. Section 4 delves into the countermeasures against web tracking and mechanisms that have been proposed to allow users to control and limit tracking, as well as studies into end-user perspectives on tracking. Section 5 focuses on tracking on "smart" devices including smartphones and the Internet of

Reuben Binns (2022), "Tracking on the Web, Mobile and the Internet of Things", Foundations and Trends® in Web Science: Vol. 8, No. 1–2, pp 1–113. DOI: 10.1561/1800000029.

Things. Section 6 covers emerging issues affecting the future of tracking across these different platforms.

1

Introduction

A working definition of tracking which aligns with the focus of this monograph was provided by the World Wide Web Consortium (W3C)'s Tracking Protection Working Group in 2019:[1]

> Tracking is the collection of data regarding a particular user's activity across multiple distinct contexts and the retention, use, or sharing of data derived from that activity outside the context in which it occurred. A context is a set of resources that are controlled by the same party or jointly controlled by a set of parties.

While this definition is proposed within the context of the web, it could meaningfully be applied to other technologies and platforms such as mobile apps and other devices connected to the internet (the so-called Internet of Things or IoT). As we shall see later, similar issues arise across all three.

Let us begin by unpacking this definition with an example. Imagine Alice visits the website of a book shop and browses through their collection of wildlife books. She then goes to her favourite search engine

[1] https://perma.cc/3HXA-F47U.

and searches for articles about climate change policy. She sees a link to a speech made in Parliament referring to the climate crisis, which she clicks on and reads. Data about Alice's activity—browsing the book site, entering search terms, slowly scrolling through the parliamentary records—can be and almost certainly is being collected in some form by the organisations behind these websites and services. Such collection would not, by itself, be considered "tracking", so long as data collected within one context stayed within that context. But if an interested party somehow collates these different data points—e.g., her book shop browsing is somehow connected to data about her search terms, or what she was looking at on the parliament website—then this would count as tracking according to the above definition.

There are many different ways this tracking could be happening; many different parties that might be involved; and many different purposes for doing so. Alice might be tracked by her own browser, which monitors her browsing behaviour to personalise web content recommendations to her on the web and target her on other platforms (e.g., sponsored posts on a social network). She might be tracked by the search engine, which builds a picture of which search results Alice actually clicks on, so that the kinds of sites she visits show up higher in her personalised search results next time. Or she might be tracked by an advertising technology (adtech) company, whose tracking capabilities are bundled up in the code embedded by websites to display adverts and generate revenue. This enables the adtech company, who Alice has probably never heard of, to target ads to Alice based on her past behaviour on multiple different websites. Some of these vectors for tracking—the browser, the search engine, the adtech company—might also be owned and operated by the same company, enabling it to track Alice's activities in multiple ways.

With the advent of smartphones and internet of things devices, the vectors for tracking have increased; now Alice might be tracked in physical space by the apps (and operating system) accessing the GPS system on her phone, and her conversations might be listened in on by the smart speaker in her living room. All of this activity is increasingly tied together across these different devices to build ever-more detailed and proliferating personal profiles.

The term "tracking" is used to mean different things in a range of contexts, including state surveillance, public health, policing and elsewhere. This monograph primarily focuses on tracking as a near-ubiquitous commercial practice which emerged through a symbiotic (or arguably, parasitic) relationship with websites, mobile apps and other internet-based services. The tracking infrastructure embedded in modern devices provides deep, intimate portraits of our lives which is already routinely used to persuade and discriminate between consumers [68]. It goes further than the most intrusive forms of government surveillance that existed before it, relying not on manual, human listening but rather on automated data capture or what Roger Clarke calls "dataveillance" [71]. Tracking could well be considered the workhorse of what some have called "surveillance capitalism"; without it, the vast wealth and power of large digital platforms would not have been possible [120], [334]. This monograph focuses primarily on tracking in the European and North American context, but tracking has developed differently in different parts of the world [122], [233], and is more or less integrated within systems of state control and surveillance under different regimes [274], [316], [320], [329].

The remainder of this monograph is structured as follows. Section 1 introduces the concept of tracking. Section 2 provides a short history of the major developments of tracking on the web. Section 3 presents research covering the detection, measurement and analysis of web tracking technologies. Section 4 delves into the countermeasures against web tracking and mechanisms that have been proposed to allow users to control and limit tracking, as well as studies into end-user perspectives on tracking. Section 5 focuses on tracking on "smart" devices including smartphones and the Internet of Things. Section 6 covers emerging issues affecting the future of tracking across these different platforms.

References

[1] A. Acar, H. Fereidooni, T. Abera, A. K. Sikder, M. Miettinen, H. Aksu, M. Conti, A.-R. Sadeghi, and A. S. Uluagac, "Peek-a-boo: I see your smart home activities, even encrypted!" *arXiv preprint arXiv:1808.02741*, 2018.

[2] G. Acar, C. Eubank, S. Englehardt, M. Juarez, A. Narayanan, and C. Diaz, "The web never forgets: Persistent tracking mechanisms in the wild," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ACM, pp. 674–689, 2014.

[3] Y. Acar, S. Fahl, and M. L. Mazurek, "You are not your developer, either: A research agenda for usable security and privacy research beyond end users," in *2016 IEEE Cybersecurity Development (SecDev)*, IEEE, pp. 3–8, 2016.

[4] J. P. Achara, G. Acs, and C. Castelluccia, "On the unicity of smartphone applications," in *Proceedings of the 14th ACM Workshop on Privacy in the Electronic Society*, pp. 27–36, 2015.

[5] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," *Science*, vol. 347, no. 6221, pp. 509–515, 2015.

[6] A. Acquisti, C. R. Taylor, and L. Wagman, "The economics of privacy," *Journal of Economic Literature*, vol. 52, no. 2, 2016.

[7] Y. Agarwal and M. Hall, "ProtectMyPrivacy: Detecting and mitigating privacy leaks on iOS devices using crowdsourcing," en, in *Proceeding of the 11th Annual International Conference on Mobile Systems, Applications, and Services - MobiSys '13*, p. 97, Taipei, Taiwan: ACM Press, 2013.

[8] N. Agrawal, R. Binns, M. Van Kleek, K. Laine, and N. Shadbolt, "Exploring design and governance challenges in the development of privacy-preserving computation," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pp. 1–13, 2021.

[9] I. E. Akkus, R. Chen, M. Hardt, P. Francis, and J. Gehrke, "Non-tracking web analytics," in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, pp. 687–698, 2012.

[10] M. Alrizah, S. Zhu, X. Xing, and G. Wang, "Errors, misunderstandings, and attacks: Analyzing the crowdsourcing process of ad-blocking systems," in *Proceedings of the Internet Measurement Conference*, pp. 230–244, 2019.

[11] I. Altman, "The environment and social behavior: Privacy, personal space, territory, and crowding," 1975.

[12] P. America, "Chilling effects: NSA surveillance drives US writers to self-censor," New York: PEN American Center, 2013.

[13] American Association of Advertising Agencies, Association of National Advertisers, Council of Better Business Bureaus, Direct Marketing Association, and the Interactive Advertising Bureau, "Self-regulatory principles for online behavioral advertising," 2010.

[14] R. Amos, G. Acar, E. Lucherini, M. Kshirsagar, A. Narayanan, and J. Mayer, "Privacy policies over time: Curation and analysis of a million-document dataset," in *Proceedings of the Web Conference 2021*, pp. 2165–2176, 2021.

[15] J. Anderson, J. Bonneau, and F. Stajano, "Inglorious installers: Security in the application marketplace.," in *WEIS*, Citeseer, 2010.

[16] N. Andriamilanto, T. Allard, and G. Le Guelvouit, "'Guess who?' large-scale data-centric study of the adequacy of browser fingerprints for web authentication," in *International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, Springer, pp. 161–172, 2020.

[17] AppsFlyer, Initial data indicates ATT opt-in rates are much higher than anticipated – at least 41%, 2021, URL: https://www.appsflyer.com/blog/trends-insights/att-opt-in-rates-higher/.

[18] N. Apthorpe, Y. Shvartzshnaider, A. Mathur, D. Reisman, and N. Feamster, "Discovering smart home internet of things privacy norms using contextual integrity," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 2, no. 2, 2018.

[19] Article 29 Working Party, Article 29 data protection working party guidelines on automated individual decision-making and profiling for the purposes of regulation 2016/679 2017, 2017.

[20] S. Arzt, S. Rasthofer, C. Fritz, E. Bodden, A. Bartel, J. Klein, Y. Le Traon, D. Octeau, and P. McDaniel, "Flowdroid: Precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for android apps," *ACM SIGPLAN Notices*, vol. 49, no. 6, pp. 259–269, 2014.

[21] H. Assal and S. Chiasson, "'think secure from the beginning': A survey with software developers," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*, pp. 1–13, ACM Press, 2019.

[22] M. Ayenson, D. Wambach, A. Soltani, N. Good, and C. Hoofnagle, "Flash cookies and privacy ii: Now with html5 and etag respawning," *Available at SSRN 1898390*, 2011.

[23] R. Balebako, A. Marsh, J. Lin, J. Hong, and L. Faith Cranor, "The privacy and security behaviors of smartphone app developers," in *Proceedings 2014 Workshop on Usable Security*, Internet Society, 2014. tex.ids: balebako_privacy_2014.

[24] L. Barkhuus, "The mismeasurement of privacy: Using contextual integrity to reconsider privacy in HCI," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, pp. 367–376, 2012.

[25] S. Barocas and H. Nissenbaum, "On notice: The trouble with notice and consent," in *Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information*, 2009.

[26] D. Barua, J. Kay, and C. Paris, "Viewing and controlling personal sensor data: What do users want?" In *International Conference on Persuasive Technology*, Springer, pp. 15–26, 2013.

[27] L. Baruh, E. Secinti, and Z. Cemalcilar, "Online privacy concerns and privacy management: A meta-analytical review," *Journal of Communication*, vol. 67, no. 1, pp. 26–53, 2017.

[28] M. A. Bashir, S. Arshad, E. Kirda, W. Robertson, and C. Wilson, "How tracking companies circumvented ad blockers using websockets," in *Proceedings of the Internet Measurement Conference 2018*, pp. 471–477, 2018.

[29] M. A. Bashir, S. Arshad, W. K. Robertson, and C. Wilson, "Tracing information flows between ad exchanges using retargeted ads.," in *USENIX Security Symposium*, pp. 481–496, 2016.

[30] M. A. Bashir and C. Wilson, "Diffusion of user tracking data in the online advertising ecosystem," *Proceedings on Privacy Enhancing Technologies*, vol. 2018, no. 4, pp. 85–103, 2018.

[31] L. Batyuk, M. Herpich, S. A. Camtepe, K. Raddatz, A.-D. Schmidt, and S. Albayrak, "Using static analysis for automatic assessment and mitigation of unwanted and malicious activities within android applications," in *Malicious and Unwanted Software (MALWARE), 2011 6th International Conference on*, IEEE, pp. 66–72, 2011.

[32] J. Bau, J. Mayer, H. Paskov, and J. C. Mitchell, "A promising direction for web tracking countermeasures," *Proceedings of W2SP*, 2013.

[33] E. Bayamiloglu, I. Baraliuc, L. Janssens, and M. Hildebrandt, *Being Profiled: Cogitas Ergo Sum*. Amsterdam University Press, 2018.

[34] K. Beioley, "UK, German and Australian regulators unify against big tech," *Financial Times*, 2021.

[35] S. Bellman, E. J. Johnson, S. J. Kobrin, and G. L. Lohse, "International differences in information privacy concerns: A global survey of consumers," *The Information Society*, vol. 20, no. 5, pp. 313–324, 2004.

[36] Z. Benenson, F. Gassmann, and L. Reinfelder, "Android and iOS users' differences concerning security and privacy," in *CHI '13 Extended Abstracts on Human Factors in Computing Systems on - CHI EA '13*, p. 817, Paris, France: ACM Press, 2013.

[37] J. Bennett, J. Bennett, and N. Strange, "Introduction: The utopia of independent media: Independence, working with freedom and working for free," *Media Independence: Working with Freedom or Working for Free*, pp. 1–28, 2015.

[38] C. Benninger, "Ajax storage: A look at flash cookies and internet explorer persistence," *Foundstone Professional Services & Education, McAfee*, 2006.

[39] A. R. Beresford, D. Kübler, and S. Preibusch, "Unwillingness to pay for privacy: A field experiment," *Economics Letters*, vol. 117, no. 1, pp. 25–27, 2012.

[40] R. Berjon, "The fiduciary duties of user agents," *Available at SSRN 3827421*, 2021.

[41] T. Berners-Lee, *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor*. Harper San Francisco, 1999.

[42] B. Bezawada, M. Bachani, J. Peterson, H. Shirazi, I. Ray, and I. Ray, "IoTSense: Behavioral fingerprinting of IoT devices," *arXiv preprint arXiv:1804.03852*, 2018.

[43] N. Bielova, "Survey on javascript security policies and their enforcement mechanisms in a web browser," *The Journal of Logic and Algebraic Programming*, vol. 82, no. 8, pp. 243–262, 2013.

[44] I. Bilogrevic and M. Ortlieb, "If you put all the pieces together...: Attitudes towards data combination and sharing across services and companies," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, ACM, pp. 5215–5227, 2016.

[45] R. Binns, U. Lyngs, M. Van Kleek, J. Zhao, T. Libert, and N. Shadbolt, "Third party tracking in the mobile ecosystem," *WebSci '18: 10th ACM Conference on Web Science*, 2018.

[46] R. Binns and E. Bietti, "Dissolving privacy, one merger at a time: Competition, data and third party tracking," vol. 36, p. 105 369,

[47] R. Binns, J. Zhao, M. V. Kleek, and N. Shadbolt, "Measuring third-party tracker power across web and mobile," *ACM Trans. Internet Technol.*, vol. 18, no. 4, pp. 1–22, 2018.

[48] R. Binns, J. Zhao, M. Van Kleek, and N. Shadbolt, "Measuring third party tracker power across web and mobile," *ACM Trans. Internet Technol.*, 2018.

[49] T. Book and D. S. Wallach, "A case of collusion: A study of the interface between ad libraries and their apps," in *Proceedings of Workshop on Security and Privacy in Smartphones & Mobile Devices*, ACM, pp. 79–86, 2013.

[50] T. Book and D. S. Wallach, "An empirical study of mobile ad targeting," *arXiv preprint arXiv:1502.06577*, 2015.

[51] F. J. Z. Borgesius, "Singling out people without knowing their names–behavioural targeting, pseudonymous data, and the new data protection regulation," *Computer Law & Security Review*, vol. 32, no. 2, pp. 256–271, 2016.

[52] F. Z. Borgesius, "The breyer case of the court of justice of the european union: Ip addresses and the personal data definition," *Eur. Data Prot. L. Rev.*, vol. 3, p. 130, 2017.

[53] E. Bott, "Why do not track is worse than a miserable failure," 2012.

[54] F. Braun, "Origin policy enforcement in modern browsers," PhD Thesis, Diploma Thesis, 2012.

[55] I. Brown *et al.*, "Interoperability as a tool for competition regulation," *OpenForum Academy*, 2020.

[56] F. Brunton and H. Nissenbaum, *Obfuscation: A User's Guide for Privacy and Protest*. Mit Press, 2015.

[57] G. Buttarelli, "This is not an article on data protection and competition law," *CPI Antitrust Chronicle*, 2019.

[58] C. Castelluccia, S. Grumbach, L. Olejnik, *et al.*, "Data harvesting 2.0: From the visible to the invisible web," in *The Twelfth Workshop on the Economics of Information Security*, 2013.

[59] C. Castelluccia, L. Olejnik, and T. Minh-Dung, "Selling off privacy at auction," *Network and Distributed System Security Symposium (NDSS)*, 2014.

[60] F. H. Cate, "The failure of fair information practice principles," in *Consumer Protection in the Age of the 'Information Economy'*, Routledge, 2006.

[61] G. Chalhoub, M. J. Kraemer, N. Nthala, and I. Flechais, "'It did not give me an option to decline': A longitudinal analysis of the user experience of security and privacy in smart home products," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pp. 1–16, 2021.

[62] F. Chanchary and S. Chiasson, "User perceptions of sharing, advertising, and tracking," in *Eleventh Symposium on Usable Privacy and Security ({SOUPS} 2015)*, pp. 53–67, 2015.

[63] A. Chandler and M. Wallace, "Using piwik instead of google analytics at the cornell university library," *The Serials Librarian*, vol. 71, no. 3–4, pp. 173–179, 2016.

[64] D. N. Chin, "Knome: Modeling what the user knows in uc," in *User Models in Dialog Systems*, Springer, 1989, pp. 74–107.

[65] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, "Private information retrieval," in *Proceedings of IEEE 36th Annual Foundations of Computer Science*, IEEE, pp. 41–50, 1995.

[66] H. K. Chowdhury, N. Parvin, C. Weitenberner, and M. Becker, "Consumer attitude toward mobile advertising in an emerging market: An empirical study," *International Journal of Mobile Marketing*, vol. 1, no. 2, 2006.

[67] C. G. Christians, Normative theories of the media: Journalism in democratic societies, vol. 117. University of Illinois Press, 2009.

[68] W. Christl, K. Kopp, and P. U. Riechert, "How companies use personal data against people," *Automated Disadvantage, Personalized Persuasion, and the Societal Ramifications of the Commercial Use of Personal Information.* Wien: Cracked Labs, 2017.

[69] G. Chu, N. Apthorpe, and N. Feamster, "Security and privacy analyses of internet of things children's toys," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 978–985, 2018.

[70] H. Chung, M. Iorga, J. Voas, and S. Lee, "Alexa, can i trust you?" *Computer*, vol. 50, no. 9, p. 100, 2017.

[71] R. Clarke, "Information technology and dataveillance," *Communications of the ACM*, vol. 31, no. 5, pp. 498–512, 1988.

[72] R. Clayton and T. Mansfield, "A study of whois privacy and proxy service abuse," in *Proceedings (Online) of the 13th Workshop on Economics of Information Security, State College, PA (June 2014)*, 2014.

[73] J. Cobbe and J. Singh, "Artificial intelligence as a service: Legal responsibilities, liabilities, and policy challenges," *Forthcoming in Computer Law & Security Review*, 2021.

[74] J. Colnago, Y. Feng, T. Palanivel, S. Pearman, M. Ung, A. Acquisti, L. F. Cranor, and N. Sadeh, "Informing the design of a personalized privacy assistant for the internet of things," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pp. 1–13, 2020.

[75] J. Cook, R. Nithyanand, and Z. Shafiq, "Inferring tracker-advertiser relationships in the online advertising ecosystem using header bidding," *Proceedings on Privacy Enhancing Technologies*, vol. 2020, no. 1, pp. 65–82, 2020.

[76] E. Costanza, J. E. Fischer, J. A. Colley, T. Rodden, S. D. Ramchurn, and N. R. Jennings, "Doing the laundry with agents: A field trial of a future smart energy system in the home," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, pp. 813–822, 2014.

[77] A. Crabtree, T. Lodge, J. Colley, C. Greenhalgh, K. Glover, H. Haddadi, Y. Amar, R. Mortier, Q. Li, J. Moore, *et al.*, "Building accountability into the internet of things: The iot databox model," *Journal of Reliable Intelligent Environments*, vol. 4, no. 1, pp. 39–55, 2018.

[78] L. F. Cranor, "Agents of choice: Tools that facilitate notice and choice about web site data practices," *arXiv preprint cs/0001011*, 2000.

[79] L. F. Cranor, M. Arjula, and P. Guduru, "Use of a p3p user agent by early adopters," in *Proceedings of the 2002 ACM Workshop on Privacy in the Electronic Society*, pp. 1–10, 2002.

[80] L. F. Cranor, A. L. Durity, A. Marsh, and B. Ur, "Parents' and teens' perspectives on privacy in a technology-filled world," in *Symposium on Usable Privacy and Security (SOUPS)*, 2014.

[81] L. F. Cranor, P. G. Leon, and B. Ur, "A large-scale evaluation of us financial institutions' standardized privacy notices," *ACM Transactions on the Web (TWEB)*, vol. 10, no. 3, p. 17, 2016.

[82] L. F. Cranor, J. Reagle, and M. S. Ackerman, *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy*. Cambridge, MA: MIT Press, 2000.

[83] J. Crussell, R. Stevens, and H. Chen, "Madfraud: Investigating ad fraud in android applications," in *Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, and Services*, pp. 123–134, 2014.

[84] M. J. Culnan, "Protecting privacy online: Is self-regulation working?" *Journal of Public Policy & Marketing*, vol. 19, no. 1, pp. 20–26, 2000.

[85] A. Das, G. Acar, N. Borisov, and A. Pradeep, "The web's sixth sense: A study of scripts accessing smartphone sensors," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1515–1532, 2018.

[86] A. Das, N. Borisov, and M. Caesar, "Tracking mobile web users through motion sensors: Attacks and defenses.," in *NDSS*, 2016.

[87] D. Davidson, M. Fredrikson, and B. Livshits, "Morepriv: Mobile os support for application personalization and privacy," in *Proceedings of the 30th Annual Computer Security Applications Conference*, pp. 236–245, 2014.

[88] W. Davis, *Kissmetrics Finalizes Supercookies Settlement*, 2013.

[89] Y.-A. De Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel, "Unique in the crowd: The privacy bounds of human mobility," *Scientific Reports*, vol. 3, no. 1, pp. 1–5, 2013.

[90] M. Degeling and J. Nierhoff, "Tracking and tricking a profiler: Automated measuring and influencing of bluekai's interest profiling," in *Proceedings of the 2018 Workshop on Privacy in the Electronic Society*, pp. 1–13, 2018.

[91] L. Desimpelaere, L. Hudders, and D. Van de Sompel, "Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior," *Computers in Human Behavior*, vol. 110, p. 106 382, 2020.

[92] L. Determann, Z. J. Ruan, T. Gao, and J. Tam, "China's draft personal information protection law," *Journal of Data Protection & Privacy*, vol. 4, no. 3, pp. 235–259, 2021.

[93] J. Deville, "Digital subprime: Tracking the credit trackers," *The Sociology of Debt*, vol. 145, 2019.

[94] Digital advertising industry warns against misguided EU Regulation—IAB Europe, 2020, URL: https://iabeurope.eu/all-news/digital-advertising-industrywarns-against-misguided-eu-regulation/.

[95] Y. Dimova, G. Acar, L. Olejnik, W. Joosen, and T. Van Goethem, "The cname of the game: Large-scale analysis of dns-based tracking evasion," *arXiv preprint arXiv:2102.09301*, 2021.

[96] P. Dixon, "The network advertising initiative: Failing at consumer protection and at self-regulation," *World Privacy Forum*, vol. 15, 2007.

[97] P. Dourish and K. Anderson, "Collective information practice: Exploring privacy and security as social and cultural phenomena," *Human-Computer Interaction*, vol. 21, no. 3, pp. 319–342, 2006.

[98] L. Dowthwaite, H. Creswick, V. Portillo, J. Zhao, M. Patel, E. P. Vallejos, A. Koene, and M. Jirotka, "'It's your private information. It's your life.' Young people's views of personal data use by online technologies," in *Proceedings of the Interaction Design and Children Conference*, pp. 121–134, 2020.

[99] N. A. Draper, "From privacy pragmatist to privacy resigned: Challenging narratives of rational choice in digital privacy debates," *Policy & Internet*, vol. 9, no. 2, pp. 232–251, 2017.

[100] E. D. E. Dwoskin, "Data broker removes rape-victims list after journal inquiry," *Wall Street Journal*, 2013.

[101] P. Eckersley, "How unique is your web browser?" In *Privacy Enhancing Technologies Symposium*, Springer, pp. 1–18, 2010.

[102] B. Edelman, "Does google leverage market power through tying and bundling?" *Journal of Competition Law and Economics*, vol. 11, no. 2, pp. 365–400, 2015.

[103] B. G. Edelman and D. Geradin, "Android and competition law: Exploring and assessing google's practices in mobile," 2016.

[104] M. Egele, C. Kruegel, E. Kirda, and G. Vigna, "Pios: Detecting privacy leaks in iOS applications.," in *NDSS*, pp. 177–183, 2011.

[105] M. Egele, C. Kruegel, E. Kirda, and G. Vigna, "Pios: Detecting privacy leaks in iOS applications," in *Proceedings of NDSS 2018,* 1, 2011.

[106] S. Egelman, A. P. Felt, and D. Wagner, "Choice architecture and smartphone privacy: There'sa price for that," in *The Economics of Information Security and Privacy*, Springer, 2013, pp. 211–236.

[107] A. Ekambaranathan, J. Zhao, and M. Van Kleek, "'Money makes the world go around': Identifying barriers to better privacy in children's apps from developers' perspectives," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pp. 1–15, 2021.

[108] P. Emami-Naeini, S. Bhagavatula, H. Habib, M. Degeling, L. Bauer, L. F. Cranor, and N. Sadeh, "Privacy expectations and preferences in an iot world," in *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pp. 399–412, 2017.

[109] W. Enck, P. Gilbert, S. Han, V. Tendulkar, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth, "Taintdroid: An information-flow tracking system for realtime privacy monitoring on smartphones," *ACM Transactions on Computer Systems (TOCS)*, vol. 32, no. 2, p. 5, 2014.

[110] S. Englehardt, C. Eubank, P. Zimmerman, D. Reisman, and A. Narayanan, "Web privacy measurement: Scientific principles, engineering platform, and new results," vol. 8, pp. 20–62, 2014. URL: http://randomwalker.info/publications/WebPrivacyMeasurement.pdf.

[111] S. Englehardt and A. Narayanan, "Online tracking: A 1-million-site measurement and analysis," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ACM, pp. 1388–1401, 2016.

[112] S. Englehardt and A. Narayanan, "Online tracking: A 1-million-site measurement and analysis," in *Proceedings of ACM Computer and Communications Security 2016*, 2016.

[113] S. Englehardt, D. Reisman, C. Eubank, P. Zimmerman, J. Mayer, A. Narayanan, and E. W. Felten, "Cookies that give you away: The surveillance implications of web tracking," in *Proceedings of the 24th International Conference on World Wide Web*, International World Wide Web Conferences Steering Committee, pp. 289–299, 2015.

[114] M. Eslami, S. R. Krishna Kumaran, C. Sandvig, and K. Karahalios, "Communicating algorithmic process in online behavioral advertising," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pp. 1–13, 2018.

[115] C. Eubank, M. Melara, D. Perez-Botero, and A. Narayanan, "Shining the floodlights on mobile web tracking—A privacy survey," in *Proceedings of the IEEE Workshop on Web*, Citeseer, vol. 2, 2013.

[116] A. P. Felt, S. Egelman, and D. Wagner, "I've got 99 problems, but vibration ain't one: A survey of smartphone users' concerns," in *Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, ACM, pp. 33–44, 2012.

[117] E. W. Felten and M. A. Schneider, "Timing attacks on web privacy," in *Proceedings of the 7th ACM Conference on Computer and Communications Security*, ACM, pp. 25–32, 2000.

[118] D. Fifield and S. Egelman, "Fingerprinting web users through font metrics," in *International Conference on Financial Cryptography and Data Security*, Springer, pp. 107–124, 2015.

[119] Flurry, iOS 14.5 opt-in Rate—Daily updates since launch, 2021. URL: https://www.flurry.com/blog/ios-14-5-opt-in-rate-att-restricted-app-tracking-transparency-worldwide-us-daily-latest-update/.

[120] J. B. Foster and R. W. McChesney, "Surveillance capitalism: Monopoly-finance capital, the military-industrial complex, and the digital age," *Monthly Review*, vol. 66, no. 3, p. 1, 2014.

[121] I. Fouad, N. Bielova, A. Legout, and N. Sarafijanovic-Djukic, "Missed by filter lists: Detecting unknown third-party trackers with invisible pixels," *arXiv preprint arXiv:1812.01514*, 2018.

[122] N. Fruchter, H. Miao, S. Stevenson, and R. Balebako, "Variations in tracking in relation to geographic location," *arXiv preprint arXiv:1506.04103*, 2015.

[123] G. G. Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, vol. 16. Springer Science & Business, 2014.

[124] O. H. Gandy Jr, *The Panoptic Sort: A Political Economy of Personal Information. Critical Studies in Communication and in the Cultural Industries.* ERIC, 1993.

[125] D. Garcia, "Leaking privacy and shadow profiles in online social networks," *Science Advances*, vol. 3, no. 8, e1701172, 2017.

[126] R. Gellman, "Fair information practices: A basic history," *Self Published*, 2016.

[127] N. Gerber, P. Gerber, H. Drews, E. Kirchner, N. Schlegel, T. Schmidt, and L. Scholz, "Foxit: Enhancing mobile users' privacy behavior by increasing knowledge and awareness," in *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust*, ACM, pp. 53–63, 2018.

[128] R. Gomer, E. M. Rodrigues, N. Milic-Frayling, and mc schraefel, "Network analysis of third party tracking: User exposure to tracking cookies through search," in *2013 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT)*, IEEE, vol. 1, pp. 549–556, 2013.

[129] R. Gonzalez, L. Jiang, M. Ahmed, M. Marciel, R. Cuevas, H. Metwalley, and S. Niccolini, "The cookie recipe: Untangling the use of cookies in the wild," in *2017 Network Traffic Measurement and Analysis Conference (TMA)*, IEEE, pp. 1–9, 2017.

[130] Google Advertising ID, URL: https://support.google.com/googleplay/android-developer/answer/6048248#zippy=%2Ctargeting-devices-without-an-advertising-id%2Cpersistent-identifiers-including-android-id.

[131] M. Goulden, B. Bedwell, S. Rennick-Egglestone, T. Rodden, and A. Spence, "Smart grids, smart users? The role of the user in demand side management," *Energy Research & Social Science*, vol. 2, pp. 21–29, 2014.

[132] C. M. Gray, C. Santos, N. Bielova, M. Toth, and D. Clifford, "Dark patterns and the legal requirements of consent banners: An interaction criticism perspective," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pp. 1–18, 2021.

[133] R. M. Gray, *Entropy and Information Theory*. Springer Science & Business Media, 2011.

[134] M. Green, W. Ladd, and I. Miers, "A protocol for privately reporting ad impressions at scale," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1591–1601, 2016.

[135] J. Grossklags and N. Good, "Empirical studies on software notices to inform policy makers and usability designers," in *International Conference on Financial Cryptography and Data Security*, Springer, pp. 341–355, 2007.

[136] E. Grünewald and F. Pallas, "Tilt: A gdpr-aligned transparency information language and toolkit for practical privacy engineering," in *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, pp. 636–646, 2021.

[137] S. Gürses and B. Berendt, "Pets in the surveillance society: A critical review of the potentials and limitations of the privacy as confidentiality paradigm," in *Data Protection in a Profiled World*, Springer, 2010, pp. 301–321.

[138] H. Haddadi, P. Hui, T. Henderson, and I. Brown, "Targeted advertising on the handset: Privacy and security challenges," *In Pervasive Advertising*, pp. 119–137, 2011.

[139] C. Han, I. Reyes, Á. Feal, J. Reardon, P. Wijesekera, A. Elazari, K. A. Bamberger, and S. Egelman, "The price is (not) right: Comparing privacy in free and paid apps," p. 21, 2020.

[140] J. Han, Q. Yan, D. Gao, J. Zhou, and R. H. Deng, "Comparing mobile privacy protection through cross-platform applications," in *Proceedings 2013 Network and Distributed System Security Symposium*, p. 16, Internet Society, 2013.

[141] D. Hedin, A. Birgisson, L. Bello, and A. Sabelfeld, "Jsflow: Tracking information flow in javascript and its APIs," in *Proceedings of the 29th Annual ACM Symposium on Applied Computing*, pp. 1663–1671, 2014.

[142] R. Helles, S. Lomborg, and S. S. Lai, "Infrastructures of tracking: Mapping the ecology of third-party services across top sites in the eu," *New Media & Society*, vol. 22, no. 11, pp. 1957–1975, 2020.

[143] M. Hildebrandt and S. Gutwirth, *Profiling the European citizen*. Springer, 2008.

[144] M. Hils, D. W. Woods, and R. Böhme, "Privacy preference signals: Past, present and future," *Proceedings on Privacy Enhancing Technologies*, vol. 2021.4, pp. 249–269, 2021.

[145] C. J. Hoofnagle, "Big brother's little helpers: How choicepoint and other commercial data brokers collect and package your data for law enforcement," *North Carolina Journal of International Law and Commercial Regulation*, vol. 29, p. 595, 2003.

[146] C. Hoofnagle, J. Urban, and S. Li, "Privacy and modern advertising: Most us internet users want "Do Not Track" to stop collection of data about their online activities," in *Amsterdam Privacy Conference*, 2012.

[147] D. C. Howe and H. Nissenbaum, "Engineering privacy and protest: A case study of adnauseam.," in *IWPE@ SP*, pp. 57–64, 2017.

[148] X. Hu, G. S. de Tangil, and N. Sastry, "Multi-country study of third party trackers from real browser histories," in *2020 IEEE European Symposium on Security and Privacy (EuroS&P)*, IEEE, pp. 70–86, 2020.

[149] T. Hupperich, D. Maiorca, M. Kührer, T. Holz, and G. Giacinto, "On the robustness of mobile device fingerprinting: Can mobile users escape modern web-tracking mechanisms?" In *Proceedings of the 31st Annual Computer Security Applications Conference*, pp. 191–200, 2015.

[150] P. Hustinx, Privacy and competitiveness in the age of big data: Preliminary opinion of the european data protection supervisor, 2014.

[151] T. Hwang, "Subprime attention crisis," *New York: FSG Originals x Logic*, 2020.

[152] M. Ikram, H. J. Asghar, M. A. Kaafar, B. Krishnamurthy, and A. Mahanti, "Towards seamless tracking-free web: Improved detection of trackers via one-class learning," *arXiv preprint arXiv:1603.06289*, 2016.

[153] International Association of Privacy Professionals, Apple's ATT rollout presents uncertain path for adtech, 2021. URL: https://iapp.org/news/a/apples-att-rollout-presents-uncertain-path-for-adtech/.

[154] U. Iqbal, S. Englehardt, and Z. Shafiq, "Fingerprinting the fingerprinters: Learning to detect browser fingerprinting behaviors," *arXiv preprint arXiv:2008.04480*, 2020.

[155] U. Iqbal, Z. Shafiq, and Z. Qian, "The ad wars: Retrospective measurement and analysis of anti-adblock filter lists," in *Proceedings of the 2017 Internet Measurement Conference*, pp. 171–183, 2017.

[156] U. Iqbal, P. Snyder, S. Zhu, B. Livshits, Z. Qian, and Z. Shafiq, "Adgraph: A graph-based approach to ad and tracker blocking," in *2020 IEEE Symposium on Security and Privacy (SP)*, IEEE, pp. 763–776, 2020.

[157] C. Jackson, A. Bortz, D. Boneh, and J. C. Mitchell, "Protecting browser state from web privacy attacks," in *Proceedings of the 15th International Conference on World Wide Web*, ACM, pp. 737–744, 2006.

[158] T. Jackson, "This bug in your pc is a smart cookie," *Financial Times*, vol. 12, no. 1996, p. 15, 1996.

[159] C. Jensen and C. Potts, "Privacy policies as decision-making tools: An evaluation of online privacy notices," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 471–478, 2004.

[160] H. Jin, M. Liu, K. Dodhia, Y. Li, G. Srivastava, M. Fredrikson, Y. Agarwal, and J. I. Hong, "Why are they collecting my data? Inferring the purposes of network traffic in mobile apps," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 2, no. 4, pp. 1–27, 2018.

[161] M. L. Jones, "Cookies: A legacy of controversy," *Internet Histories*, vol. 4, no. 1, pp. 87–104, 2020.

[162] S. Kamkar, "Evercookie," 2010. URL: http://samy.pl/evercookie.

[163] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler, "'My data just goes everywhere:' User mental models of the internet and implications for privacy and security," in *Proceedings of Symposium on Usable Privacy and Security*, pp. 39–52, 2015.

[164] A. Karaj, S. Macbeth, R. Berson, and J. M. Pujol, "Whotracks.me: Monitoring the online tracking landscape at scale," *arXiv preprint arXiv:1804.08959*, 2018.

[165] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder, "A nutrition label for privacy," in *Proceedings of Symposium on Usable Privacy and Security*, ACM, p. 4, 2009.

[166] L. M. Khan, "Amazon's antitrust paradox," 2017.

[167] S. Kim and J. S. Baek, "Definitions and attributes of smart home appliances," in *Proceedings of the Design Society: International Conference on Engineering Design*, Cambridge University Press, vol. 1, pp. 2071–2080, 2019.

[168] J. King, "How come i'm allowing strangers to go through my phone? Smartphones and privacy expectations.," *Smartphones and Privacy Expectations*, 2012.

[169] P. Klasnja, S. Consolvo, T. Choudhury, R. Beckwith, and J. Hightower, "Exploring privacy concerns about personal sensing," in *International Conference on Pervasive Computing*, Springer, pp. 176–183, 2009.

[170] S. Kokolakis, "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Computers & Security*, vol. 64, pp. 122–134, 2017.

[171] K. Kollnig, R. Binns, M. Van Kleek, U. Lyngs, J. Zhao, C. Tinsman, and N. Shadbolt, "Before and after gdpr: Tracking in mobile apps," *Internet Policy Review*, vol. 10, no. 4, 2021.

[172] K. Kollnig, R. Binns, P. Dewitte, M. Van Kleek, G. Wang, D. Omeiza, H. Webb, and N. Shadbolt, "A fait accompli? An empirical study into the absence of consent to third-party tracking in androidãpps," *arXiv preprint arXiv:2106.09407*, 2021.

[173] K. Kollnig, A. Shuba, R. Binns, M. Van Kleek, and N. Shadbolt, "Are iphones really better for privacy? Comparative study of iOS and android apps," *arXiv preprint arXiv:2109.13722*, 2021.

[174] K. Kollnig, A. Shuba, M. Van Kleek, R. Binns, and N. Shadbolt, "Goodbye tracking? Impact of iOS app tracking transparency and privacy labels," in *ACM FAccT '22*, Seoul: Republic of Korea, 2022, pp. 21–24.

[175] S. Komanduri, R. Shay, G. Norcie, and B. Ur, "Adchoices-compliance with online behavioral advertising notice and choice requirements," *ISJLP*, vol. 7, p. 603, 2011.

[176] M. J. Kraemer, I. Flechais, and H. Webb, "Exploring communal technology use in the home," in *Proceedings of the Halfway to the Future Symposium 2019*, pp. 1–8, 2019.

[177] B. Krishnamurthy, K. Naryshkin, and C. Wills, "Privacy leakage vs. protection measures: The growing disconnect," in *Web 2.0 Security and Privacy Workshop*, 2011.

[178] B. Krishnamurthy and C. E. Wills, "Generating a privacy footprint on the internet," in *Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement*, ACM, pp. 65–70, 2006.

[179] B. Krupp, J. Hadden, and M. Matthews, "An analysis of web tracking domains in mobile applications," in *13th ACM Web Science Conference 2021*, pp. 291–298, 2021.

[180] P. Kumaraguru and L. F. Cranor, "Privacy indexes: A survey of westin's studies," 2005.

[181] M. Langheinrich, "To floc or not?" *IEEE Pervasive Computing*, vol. 20, no. 2, pp. 4–6, 2021.

[182] P. Laperdrix, N. Bielova, B. Baudry, and G. Avoine, "Browser fingerprinting: A survey," *ACM Transactions on the Web (TWEB)*, vol. 14, no. 2, pp. 1–33, 2020.

[183] M. Lécuyer, G. Ducoffe, F. Lan, A. Papancea, T. Petsios, R. Spahn, A. Chaintreau, and R. Geambasu, "Xray: Enhancing the web's transparency with differential correlation," in *23rd USENIX Security Symposium (USENIX Security 14)*, pp. 49–64, San Diego, CA: USENIX Association, 2014.

[184] D. Lee, R. Larose, and N. Rifon, "Keeping our network safe: a model of online protection behaviour," *Behaviour & Information Technology*, vol. 27, no. 5, pp. 445–454, 2008.

[185] H. Lee and A. Kobsa, "Understanding user privacy in internet of things environments," in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, IEEE, pp. 407–412, 2016.

[186] B. M. Leiner, V. G. Cerf, D. D. Clark, R. E. Kahn, L. Kleinrock, D. C. Lynch, J. Postel, L. G. Roberts, and S. Wolff, "A brief history of the internet," *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 5, pp. 22–31, 2009.

[187] P. G. Leon, L. F. Cranor, A. M. McDonald, and R. McGuire, "Token attempt: The misrepresentation of website privacy policies through the misuse of p3p compact policy tokens," in *Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society*, pp. 93–104, 2010.

[188] P. G. Leon, B. Ur, Y. Wang, M. Sleeper, R. Balebako, R. Shay, L. Bauer, M. Christodorescu, and L. F. Cranor, "What matters to users?: Factors that affect users' willingness to share information with online advertisers," in *Proceedings of Symposium on Usable Privacy and Security*, ACM, pp. 1–7, 2013.

[189] P. Leon, B. Ur, R. Shay, Y. Wang, R. Balebako, and L. Cranor, "Why johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, pp. 589–598, 2012.

[190] A. Lerner, A. K. Simpson, T. Kohno, and F. Roesner, "Internet jones and the raiders of the lost trackers: An archaeological study of web tracking from 1996 to 2016," in *USENIX Security Symposium*, 2016.

[191] L. Lessig, "The architecture of privacy," *Vand. J. Ent. L. Prac.*, vol. 1, p. 56, 1999.

[192] C. Leung, J. Ren, D. Choffnes, and C. Wilson, "Should you use the app for that? Comparing the privacy implications of app-and web-based online services," in *Proc. of the 16th ACM Internet Measurement Conference*, 2016.

[193] R. A. Lewis and J. M. Rao, "The unfavorable economics of measuring the returns to advertising," *Available at SSRN 2367103*, 2014.

[194] T. Libert and V. Pickard, "Think you're reading the news for free? New research shows you're likely paying with your privacy," *The Conversation*, 2015.

[195] T. Libert, "Exposing the hidden web: Third-party http requests on one million websites," *International Journal of Communication*, 2015.

[196] T. Libert, "An automated approach to auditing disclosure of third-party data collection in site privacy policies," *Proceedings of the 2018 World Wide Web Conference*, pp. 207–216, 2018.

[197] T. Libert and R. Binns, "Good news for people who love bad news: Centralization, privacy, and transparency on us news sites," in *Proceedings of the 10th ACM Conference on Web Science*, pp. 155–164, 2019.

[198] T. Libert, A. Desai, and D. Patel, "Preserving needles in the haystack: A search engine and multi-jurisdictional forensic documentation system for privacy violations on the web," Published 2021, URL: https://timlibert.me/pdf/Libert_et_al-2021-Forensic_Privacy_on_Web.pdf.

[199] T. Libert, D. Grande, and D. A. Asch, "What web browsing reveals about your health," *BMJ*, vol. 351, h5974, 2015.

[200] J. Lin, S. Amini, J. I. Hong, N. Sadeh, J. Lindqvist, and J. Zhang, "Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing," in *Proceedings of Conference on Ubiquitous Computing*, ACM, pp. 501–510, 2012.

[201] J. Lin, B. Liu, N. Sadeh, and J. I. Hong, "Modeling users' mobile app privacy preferences: Restoring usability in a sea of permission settings," in *Symposium on Usable Privacy and Security (SOUPS 2014)*, pp. 199–212, Menlo Park, CA: USENIX Association, Jul. 2014.

[202] J. Lin, B. Liu, N. Sadeh, and J. I. Hong, "Modeling users' mobile app privacy preferences: Restoring usability in a sea of permission settings," in *Symposium on Usable Privacy and Security*, pp. 199–212, 2014.

[203] B. Liu, S. Nath, R. Govindan, and J. Liu, "{*DECAF*}: Detecting and characterizing ad fraud in mobile apps," in *11th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 14)*, pp. 57–70, 2014.

[204] C. Lu, B. Liu, Y. Zhang, Z. Li, F. Zhang, H. Duan, Y. Liu, J. Q. Chen, J. Liang, Z. Zhang, S. Hao, and M. Yang, From WHOIS to WHOWAS: A large-scale measurement study of domain registration privacy under the GDPR, 2021.

[205] O. Lynskey, "Aligning data protection rights with competition law remedies? The GDPR right to data portability," *European Law Review*, vol. 42, no. 6, pp. 793–814, 2017.

[206] Z. Ma, H. Wang, Y. Guo, and X. Chen, "Libradar: Fast and accurate detection of third-party libraries in android apps," in *Proceedings of the 38th International Conference on Software Engineering Companion*, ACM, pp. 653–656, 2016.

[207] M. Madden, "Public perceptions of privacy and security in the post-snowden era," *Pew Research Center*, 2014.

[208] N. Malkin, J. Bernd, M. Johnson, and S. Egelman, "'What can't data be used for'? Privacy expectations about smart tvs in the us," in *European Workshop on Usable Security (Euro USEC)*, 2018.

[209] A. M. Mandalari, R. Kolcun, H. Haddadi, D. J. Dubois, and D. Choffnes, "Towards automatic identification and blocking of non-critical iot traffic destinations," *arXiv preprint arXiv:2003.07133*, 2020.

[210] V. Marotta, V. Abhishek, and A. Acquisti, "Online tracking and publishers' revenues: An empirical analysis," in *Workshop on the Economics of Information Security*, 2019.

[211] A. Marthews and C. E. Tucker, "Government surveillance and internet search behavior," *SSRN*, 2015.

[212] K. E. Martin and H. Nissenbaum, "Measuring privacy: An empirical test using context to expose confounding variables," *Columbia Science and Technology Law Review*, vol. 18, no. Fall, pp. 176–218, 2016.

[213] A. Mathur, J. Vitak, A. Narayanan, and M. Chetty, "Characterizing the use of browser-based blocking extensions to prevent online tracking," in *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*, pp. 103–116, 2018.

[214] C. Matte, N. Bielova, and C. Santos, "Do cookie banners respect my choice?: Measuring legal compliance of banners from iab europe's transparency and consent framework," in *2020 IEEE Symposium on Security and Privacy (SP)*, IEEE, pp. 791–809, 2020.

[215] J. R. Mayer and J. C. Mitchell, "Third-party web tracking: Policy and technology," in *IEEE Symposium on Security and Privacy*, IEEE, pp. 413–427, 2012.

[216] J. R. Mayer and J. C. Mitchell, "Third-party web tracking: Policy and technology," in *2012 IEEE Symposium on Security and Privacy*, IEEE, pp. 413–427, 2012.

[217] J. R. Mayer and A. Narayanan, "Do not track: A universal third-party web tracking opt out," *Internet Engineering Task Force*, 2011. URL: http://www.ietf.org/archive/id/draft-mayer-do-not-track-00.txt.

[218] A. M. McDonald and L. F. Cranor, "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society*, vol. 4, p. 26, 2008.

[219] E. McReynolds, S. Hubbard, T. Lau, A. Saraf, M. Cakmak, and F. Roesner, "Toys that listen: A study of parents, children, and internet-connected toys," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, ACM, pp. 5197–5207, 2017.

[220] M. F. McTear, "User modelling for adaptive computer systems: A survey of recent developments," *Artificial Intelligence Review*, vol. 7, no. 3-4, pp. 157–184, 1993.

[221] S. Meier, *Erfolgreicher Anzeigenverkauf in Mobilen Medien: Eine Empirische Analyse zu Verkaufsindikatoren im Mobile Advertising*. Springer-Verlag, 2014.

[222] G. Merzdovnik, M. Huber, D. Buhov, N. Nikiforakis, S. Neuner, M. Schmiedecker, and E. Weippl, "Block me if you can: A large-scale study of tracker-blocking tools," in *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, IEEE, pp. 319–333, 2017.

[223] A. H. Mhaidli, Y. Zou, and F. Schaub, "'"We can't live without them!" app developers' adoption of ad networks and their considerations of consumer risks," p. 21, 2019.

[224] M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A.-R. Sadeghi, and S. Tarkoma, "IoT Sentinel: Automated device-type identification for security enforcement in iot," in *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, IEEE, pp. 2177–2184, 2017.

[225] H. Mohajeri Moghaddam, G. Acar, B. Burgess, A. Mathur, D. Y. Huang, N. Feamster, E. W. Felten, P. Mittal, and A. Narayanan, "Watching you watch: The tracking ecosystem of over-the-top tv streaming devices," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 131–147, 2019.

[226] R. Montes, W. Sand-Zantman, and T. M. Valletti, "The value of personal information in markets with endogenous privacy," *Management Science*, 2015.

[227] K. Mowery and H. Shacham, "Pixel perfect: Fingerprinting canvas in html5," *Proceedings of W2SP*, pp. 1–12, 2012.

[228] A. Narayanan, J. Huey, and E. W. Felten, "A precautionary approach to big data privacy," in *Data Protection on the Move*, Springer, 2016, pp. 357–385.

[229] N. Nikiforakis, A. Kapravelos, W. Joosen, C. Kruegel, F. Piessens, and G. Vigna, "Cookieless monster: Exploring the ecosystem of web-based device fingerprinting," in *IEEE Symposium on Security and Privacy*, 2013.

[230] H. F. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, 2010.

[231] M. Nouwens, I. Liccardi, M. Veale, D. Karger, and L. Kagal, "Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence," in *CHI 2020—Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, New York: Association for Computing Machinery, 2020.

[232] T. J. OConnor, R. Mohamed, M. Miettinen, W. Enck, B. Reaves, and A.-R. Sadeghi, "Homesnitch: Behavior transparency and control for smart home iot devices," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, ACM, pp. 128–138, 2019.

[233] K. O'Hara and W. Hall, *Four Internets: Data, Geopolitics, and the Governance of Cyberspace*. Oxford University Press, 2021.

[234] E. Okoyomon, N. Samarin, P. Wijesekera, A. Elazari, N. Vallina-Rodriguez, I. Reyes, A. Feal, and S. Egelman, "On the ridiculousness of notice and consent: Contradictions in app privacy policies," in *The Workshop on Technology and Consumer Protection (ConPro '19)*, 2019.

[235] Ł. Olejnik, G. Acar, C. Castelluccia, and C. Diaz, "The leaking battery," in *Data Privacy Management, and Security Assurance*, Springer, 2015, pp. 254–263.

[236] A. Oltramari, D. Piraviperumal, F. Schaub, S. Wilson, S. Cherivirala, T. B. Norton, N. Â. C. Russell, P. Story, J. Reidenberg, and N. Sadeh, "Privonto: A semantic framework for the analysis of privacy policies," *Semantic Web*, vol. 9, pp. 1–19, May 2017.

[237] P. Papadopoulos, N. Kourtellis, and E. Markatos, "Cookie synchronization: Everything you always wanted to know but were afraid to ask," in *The World Wide Web Conference*, pp. 1432–1442, 2019.

[238] F. A. Pasquale, "Privacy, antitrust, and power," *George Mason Law Review*, vol. 20, no. 4, pp. 1009–1024, 2013.

[239] J. W. Penney, "Chilling effects: Online surveillance and wikipedia use," *Berkeley Technology Law Journal*, vol. 31, p. 117, 2016.

[240] G. Pestana, I. Querejeta-Azurmendi, P. Papadopoulos, and B. Livshits, "Themis: Decentralized and trustless ad platform with reporting integrity," *arXiv preprint arXiv:2007.05556*, 2020.

[241] Privacy International, "How apps on Android share data with Facebook," Report, 2018.

[242] A. Purington, J. G. Taft, S. Sannon, N. N. Bazarova, and S. H. Taylor, "Alexa is my new bff: Social roles, user satisfaction, and personification of the amazon echo," in *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, ACM, pp. 2853–2859, 2017.

[243] N. Purtova, "From knowing by name to personalisation: Meaning of identification under the gdpr," *Available at SSRN 3849943*, 2021.

[244] L. Qiu, Z. Zhang, Z. Shen, and G. Sun, "Apptrace: Dynamic trace on android devices," in *2015 IEEE International Conference on Communications*, IEEE, pp. 7145–7150, 2015.

[245] M. Quinlan, J. Zhao, and A. Simpson, "Connected vehicles: A privacy analysis," in *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*, Springer, pp. 35–44, 2019.

[246] A. Rao, F. Schaub, and N. Sadeh, "What do they know about me? Contents and concerns of online behavioral profiles," *arXiv preprint arXiv:1506.01675*, 2015.

[247] A. Razaghpanah, R. Nithyanand, N. Vallina-Rodriguez, S. Sundaresan, M. Allman, C. Kreibich, and P. Gill, "Apps, trackers, privacy, and regulators: A global study of the mobile tracking ecosystem," 2018.

[248] J. Reardon, Á. Feal, P. Wijesekera, A. E. B. On, N. Vallina-Rodriguez, and S. Egelman, "50 ways to leak your data: An exploration of apps' circumvention of the android permissions system," in *28th USENIX Security Symposium (USENIX Security 19)*, pp. 603–620, Santa Clara, CA: USENIX Association. August, 2019.

[249] J. Ren, D. J. Dubois, D. Choffnes, A. M. Mandalari, R. Kolcun, and H. Haddadi, "Information exposure from consumer iot devices: A multidimensional, network-informed measurement approach," in *Proceedings of the Internet Measurement Conference*, pp. 267–279, 2019.

[250] J. Ren, A. Rao, M. Lindorfer, A. Legout, and D. Choffnes, "Demo: Recon: Revealing and controlling pii leaks in mobile network traffic," in *Proceedings of the International Conference on Mobile Systems, Applications, and Services Companion,* MobiSys '16 Companion, pp. 117–117, 2016.

[251] J. Ren, A. Rao, M. Lindorfer, A. Legout, and D. Choffnes, "ReCon: Revealing and controlling PII leaks in mobile network traffic," in *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services - MobiSys '16*, pp. 361–374, Singapore, Singapore: ACM Press, 2016.

[252] I. Reyes, P. Wijesekera, J. Reardon, A. Elazari Bar On, A. Razaghpanah, N. Vallina-Rodriguez, and S. Egelman, "'Won't somebody think of the children?' Examining coppa compliance at scale," 2018.

[253] N. M. Richards, "Intellectual privacy," *Texas Law Review*, vol. 87, p. 387, 2008.

[254] T. A. Rodden, J. E. Fischer, N. Pantidi, K. Bachour, and S. Moran, "At home with agents: Exploring attitudes towards future smart energy infrastructures," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, pp. 1173–1182, 2013.

[255] M. Rotenberg, "Fair information practices and the architecture of privacy (what Larry doesn't get)," *Stanford Technology Law Review*, p. 1, 2001.

[256] N. Sanoaf Dheen, M. Sapthagiri, A. Naveenkumar, and K. Sathya Narayanan, "Network-wide range ad-blocker using raspberry pi," *International Journal of Pure and Applied Mathematics*, vol. 119, no. 10, pp. 1771–1775, 2018.

[257] C. Santos, M. Nouwens, M. Toth, N. Bielova, and V. Roca, "Consent management platforms under the gdpr: Processors and/or controllers?" In *Annual Privacy Forum*, Springer, pp. 47–69, 2021.

[258] S. Schechner, "Germany says facebook abuses market dominance to collect data," 2017.

[259] S. Schelter and J. Kunegis, "On the ubiquity of web tracking: Insights from a billion-page web crawl," *arXiv preprint arXiv:1607.07403*, 2016.

[260] J. Schwartz, "Giving the web a memory cost its users privacy," *New York Times*, vol. 4, no. 1, 2001.

[261] W. Seymour, R. Binns, P. Slovak, M. Van Kleek, and N. Shadbolt, "Strangers in the room: Unpacking perceptions of'smartness' and related ethical concerns in the home," in *Proceedings of the 2020 ACM Designing Interactive Systems Conference*, pp. 841–854, 2020.

[262] W. Seymour, M. J. Kraemer, R. Binns, and M. Van Kleek, "Informing the design of privacy-empowering tools for the connected home," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, ACM, 2020.

[263] I. Shklovski, S. D. Mainwaring, H. H. Skúladóttir, and H. Borgthorsson, "Leakiness and creepiness in app space: Perceptions of privacy and mobile app use," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, pp. 2347–2356, 2014.

[264] A. Shuba, A. Le, E. Alimpertis, M. Gjoka, and A. Markopoulou, "Antmonitor: A system for on-device mobile network monitoring and its applications," *arXiv preprint arXiv:1611.04268*, 2016.

[265] A. Shuba and A. Markopoulou, "Nomoats: Towards automatic detection of mobile tracking," *Proc. Priv. Enhancing Technol.*, vol. 2020, no. 2, pp. 45–66, 2020.

[266] S. Sivakorn, I. Polakis, and A. D. Keromytis, "The cracked cookie jar: Http cookie hijacking and the exposure of private information," in *2016 IEEE Symposium on Security and Privacy (SP)*, IEEE, pp. 724–742, 2016.

[267] Smith, Dinev, Xu, H. J. Smith, T. Dinev, and H. Xu, "Information privacy research: An interdisciplinary review," *MIS Quarterly*, vol. 35, no. 4, pp. 989–1016, 2011.

[268] P. Snyder, A. Vastel, and B. Livshits, "Who filters the filters: Understanding the growth, usefulness and efficiency of crowdsourced ad blocking," *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, vol. 4, no. 2, pp. 1–24, 2020.

[269] A. Soltani, S. Canty, Q. Mayo, L. Thomas, and C. J. Hoofnagle, "Flash cookies and privacy," in *2010 AAAI Spring Symposium Series*, 2010.

[270] A. Soltani, A. Peterson, and B. Gellman, "NSA uses Google cookies to pinpoint targets for hacking," *The Washington Post*, 2013. URL: https://www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking.

[271] Y. Song and U. Hengartner, "Privacyguard: A vpn-based platform to detect information leakage on android devices," in *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices*, pp. 15–26, 2015.

[272] Staff of Chairman Rockefeller, "A review of the data broker industry: Collection, use, and sale of consumer data for marketing purposes," *US Senate*, 2013.

[273] J. H. Steven Englehardt and A. Narayanan, "I never signed up for this! privacy implications of email tracking," *Proceedings on Privacy Enhancing Technologies*, 2018.

[274] D. Stockmann, *Media Commercialization and Authoritarian Rule in China*. Cambridge University Press, 2013.

[275] E. Stoycheff, "Under surveillance examining Facebook's spiral of silence effects in the wake of NSA internet monitoring," *Journalism & Mass Communication Quarterly,* 1077699016630255, 2016.

[276] K. Sun, C. Chen, and X. Zhang, "'Alexa, stop spying on me!' Speech privacy protection against voice assistants," in *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*, pp. 298–311, 2020.

[277] P. Swire, Protecting consumers: Privacy matters in antitrust analysis, 2007.

[278] M. Tabassum, T. Kosinski, and H. R. Lipford, "'I don't own the data': End user perceptions of smart home device data practices and risks," in *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, 2019.

[279] H. T. Tavani and J. H. Moor, "Privacy protection, control of information, and privacy-enhancing technologies," *ACM Sigcas Computers and Society*, vol. 31, no. 1, pp. 6–11, 2001.

[280] V. F. Taylor and I. Martinovic, "To update or not to update: Insights from a two-year study of android app evolution," in *ACM Asia Conference on Computer and Communications Security (ASIACCS'17)*, To appear 2017.

[281] W. B. Tesfay, P. Hofmann, T. Nakamura, S. Kiyomoto, and J. Serna, "I read but don't agree: Privacy policy benchmarking using machine learning and the eu gdpr," in *Companion Proceedings of the Web Conference 2018*, ser. WWW '18, pp. 163–166, 2018.

[282] TOSDR, "Terms of service; didn't read," 2014. URL: http://tosdr.org/.

[283] F. Tramèr, P. Dupré, G. Rusak, G. Pellegrino, and D. Boneh, "Adversarial: Perceptual ad blocking meets adversarial machine learning," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 2005–2021, 2019.

[284] M. Trevisan, S. Traverso, H. Metwalley, and M. Mellia, "Uncovering the flop of the eu cookie law," *arXiv preprint arXiv:1705.08884*, 2017.

[285] R. Trimananda, J. Varmarken, A. Markopoulou, and B. Demsky, "Pingpong: Packet-level signatures for smart home device events," *arXiv preprint arXiv:1907.11797*, 2019.

[286] M. C. Tschantz, A. Datta, A. Datta, and J. M. Wing, "A methodology for information flow experiments," in *2015 IEEE 28th Computer Security Foundations Symposium*, IEEE, pp. 554–568, 2015.

[287] I. Ullah, B. G. Sarwar, R. Boreli, S. S. Kanhere, S. Katzenbeisser, and M. Hollick, "Enabling privacy preserving mobile advertising via private information retrieval," in *2017 IEEE 42nd Conference on Local Computer Networks (LCN)*, IEEE, pp. 347–355, 2017.

[288] United States Federal Trade Commission, "FTC staff report: Self-regulatory principles for online behavioral advertising," 2009.

[289] B. Ur, P. G. Leon, L. F. Cranor, R. Shay, and Y. Wang, "Smart, useful, scary, creepy: Perceptions of online behavioral advertising," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, ACM, p. 4, 2012.

[290] T. Urban, M. Degeling, T. Holz, and N. Pohlmann, "Beyond the front page: Measuring third party dynamics in the field," in *Proceedings of the Web Conference 2020*, pp. 1275–1286, 2020.

[291] T. Urban, D. Tatang, M. Degeling, T. Holz, and N. Pohlmann, "The unwanted sharing economy: An analysis of cookie syncing and user transparency under gdpr," *arXiv preprint arXiv:1811.08660*, 2018.

[292] L. Urquhart, D. Reedman-Flint, and N. Leesakul, "Responsible domestic robotics: Exploring ethical implications of robots in the home," *Journal of Information, Communication and Ethics in Society*, 2019.

[293] C. Utz, M. Degeling, S. Fahl, F. Schaub, and T. Holz, "(un) informed consent: Studying GDPR consent notices in the field," in *Proceedings of the 2019 Acm Sigsac Conference on Computer and Communications Security*, pp. 973–990, 2019.

[294] N. Vallina-Rodriguez, S. Sundaresan, A. Razaghpanah, R. Nithyanand, M. Allman, C. Kreibich, and P. Gill, "Tracking the trackers: Towards understanding the mobile advertising and tracking ecosystem," *arXiv preprint arXiv:1609.07190*, 2016.

[295] M. Van Kleek, R. Binns, J. Zhao, A. Slack, S. Lee, D. Ottewell, and N. Shadbolt, "X-ray refine: Supporting the exploration and refinement of information exposure resulting from smartphone apps," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, ACM, pp. 1–13, ACM Press, 2018.

[296] M. Van Kleek, I. Liccardi, R. Binns, J. Zhao, D. J. Weitzner, and N. Shadbolt, "Better the devil you know: Exposing the data sharing practices of smartphone apps," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17*, pp. 5208–5220, Denver, Colorado, USA: ACM Press, 2017.

[297] M. Van Kleek, D. Murray-Rust, A. Guy, K. O'Hara, and N. Shadbolt, "Computationally mediated pro-social deception," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, ser. CHI '16, pp. 552–563, New York, NY, USA: ACM, 2016.

[298] J. Varmarken, H. Le, A. Shuba, A. Markopoulou, and Z. Shafiq, "The tv is smart and full of trackers: Measuring smart tv advertising and tracking," *Proceedings on Privacy Enhancing Technologies*, vol. 2020, no. 2, 2020.

[299] S. Vasile, D. Oswald, and T. Chothia, "Breaking all the things—A systematic survey of firmware extraction techniques for IoT devices," in *International Conference on Smart Card Research and Advanced Applications*, Springer, pp. 171–185, 2018.

[300] M. Veale and F. Z. Borgesius, "Adtech and real-time bidding under european data protection law," 2021.

[301] N. Viennot, E. Garcia, and J. Nieh, "A measurement study of google play," in *The 2014 ACM International Conference on Measurement and Modeling of Computer Systems*, ser. SIGMETRICS '14, pp. 221–233, 2014.

[302] W. Wahlster and A. Kobsa, "User models in dialog systems," *User Models in Dialog Systems*, pp. 4–34, 1989.

[303] T. Wambach and K. Bräunlich, "Retrospective study of third-party web tracking," in *Proceedings of the 2nd International Conference on Information Systems Security and Privacy*, pp. 138–145, 2016.

[304] H. Wang, Z. Liu, J. Liang, N. Vallina-Rodriguez, Y. Guo, L. Li, J. Tapiador, J. Cao, and G. Xu, "Beyond google play: A large-scale comparative study of chinese android app markets," in *Proceedings of the Internet Measurement Conference 2018*, pp. 293–307, 2018.

[305] W. H. Ware, *Records, Computers, and the Rights of Citizens: Report*, vol. 10. US Department of Health, Education & Welfare, 1973.

[306] R. Wash and E. Rader, "Too much knowledge? Security beliefs and protective behaviors among united states internet users," in *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)*, pp. 309–325, Ottawa: USENIX Association. July, 2015.

[307] E. A. Watkins, "Guide to advertising technology," 2019.

[308] R. H. Weber, "Internet of things–new security and privacy challenges," *Computer Law & Security Review*, vol. 26, no. 1, pp. 23–30, 2010.

[309] B. Weinshel, M. Wei, M. Mondal, E. Choi, S. Shan, C. Dolin, M. L. Mazurek, and B. Ur, "Oh, the places you've been! user reactions to longitudinal transparency about third-party web tracking and inferencing," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 149–166, 2019.

[310] A. Westin, *Privacy and Freedom*. London: Bodley Head, 1967.

[311] A. F. Westin, "Privacy and freedom," *Washington and Lee Law Review*, vol. 25, no. 1, p. 166, 1968.

[312] S. Wilson, F. Schaub, R. Ramanath, N. Sadeh, F. Liu, N. A. Smith, and F. Liu, "Crowdsourcing annotations for websites' privacy policies: Can it really work?" In *Proceedings of the 25th International Conference on World Wide Web*, International World Wide Web Conferences Steering Committee, pp. 133–143, 2016.

[313] A. Woodruff, V. Pihur, S. Consolvo, L. Schmidt, L. Brandimarte, and A. Acquisti, "Would a privacy fundamentalist sell their DNA for $1000... if nothing bad happened as a result? The westin categories, behavioral intentions, and consequences," in *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security*, pp. 1–18, 2014.

[314] M. Worledge and M. Bamford, "Adtech market research report".

[315] T. Wu, *The Curse of Bigness: Antitrust in the New Gilded Age*. Columbia Global Reports. OCLC: on1029205194.

[316] G. Yang, *The Power of the Internet in China: Citizen Activism Online*. Columbia University Press, 2013.

[317] X. Yao and J. Karlin, "Federated learning of cohorts," 2021. URL: https://wicg.github.io/floc/.

[318] Y. Yao, D. Lo Re, and Y. Wang, "Folk models of online behavioral advertising," in *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, pp. 1957–1969, 2017.

[319] S. Youn, "Teenagers' perceptions of online privacy and coping behaviors: A risk–benefit appraisal approach," *Journal of Broadcasting & Electronic Media*, vol. 49, no. 1, pp. 86–110, 2005.

[320] H. Yu, *Media and Cultural Transformation in China*. Routledge, 2009.

[321] Z. Yu, S. Macbeth, K. Modi, and J. M. Pujol, "Tracking the trackers," in *Proceedings of the 25th International Conference on World Wide Web*, International World Wide Web Conferences Steering Committee, pp. 121–132, 2016.

[322] S. Yuan, J. Wang, and X. Zhao, "Real-time bidding for online advertising: Measurement and analysis," in *Proceedings of the Seventh International Workshop on Data Mining for Online Advertising*, pp. 1–8, 2013.

[323] Y. Yuan, F. Wang, J. Li, and R. Qin, "A survey on real time bidding advertising," in *Proceedings of 2014 IEEE International Conference on Service Operations and Logistics, and Informatics*, IEEE, pp. 418–423, 2014.

[324] J. Zang, K. Dummit, J. Graves, P. Lisker, and L. Sweeney, "Who knows what about me? A survey of behind the scenes personal data sharing to third parties by mobile apps," *Technology Science*, vol. 30, 2015.

[325] W. Zhang, Y. Meng, Y. Liu, X. Zhang, Y. Zhang, and H. Zhu, "HoMonit: Monitoring smart home apps from encrypted traffic," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ACM, pp. 1074–1088, 2018.

[326] J. Zhao, R. Binns, M. Van Kleek, and N. Shadbolt, "Privacy languages: Are we there yet to enable user controls?" In *Proceedings of the 25th International Conference Companion on World Wide Web*, pp. 799–806, 2016.

[327] J. Zhao, G. Wang, C. Dally, P. Slovak, J. Edbrooke-Childs, M. Van Kleek, and N. Shadbolt, "I make up a silly name' understanding children's perception of privacy risks online," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pp. 1–13, 2019.

[328] S. Zheng, N. Apthorpe, M. Chetty, and N. Feamster, "User perceptions of smart home IoT privacy," in *Proc. ACM Hum.-Comput. Interact.*, vol. 2, 200:1–200:20, 2018.

[329] Y. Zhou, *Historicizing Online Politics: Telegraphy, the Internet, and Political Participation in China*. Stanford University Press, 2006.

[330] Y. Zhou and D. Evans, "Understanding and monitoring embedded web scripts," in *2015 IEEE Symposium on Security and Privacy*, IEEE, pp. 850–865, 2015.

[331] S. Zhu, X. Hu, Z. Qian, Z. Shafiq, and H. Yin, "Measuring and disrupting anti-adblockers using differential execution analysis," in *The Network and Distributed System Security Symposium (NDSS)*, 2018.

[332] S. Zimmeck, J. S. Li, H. Kim, S. M. Bellovin, and T. Jebara, "A privacy analysis of cross-device tracking," in *26th {USENIX} Security Symposium ({USENIX} Security 17)*, pp. 1391–1408, 2017.

[333] J. Zittrain, *The Future of the Internet–and How to Stop It*. Yale University Press, 2008.

[334] S. Zuboff, "Big other: Surveillance capitalism and the prospects of an information civilization," *Journal of Information Technology*, vol. 30, no. 1, pp. 75–89, 2015.