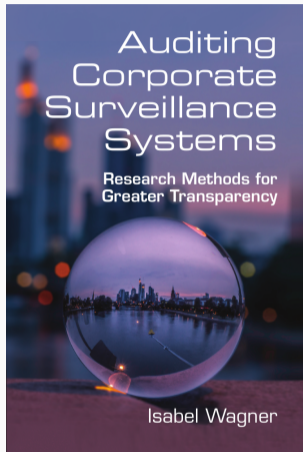


AUDITING CORPORATE SURVEILLANCE SYSTEMS

RESEARCH METHODS FOR GREATER TRANSPARENCY

Isabel Wagner

De Montfort University



Book design ©2022
by Cambridge University Press

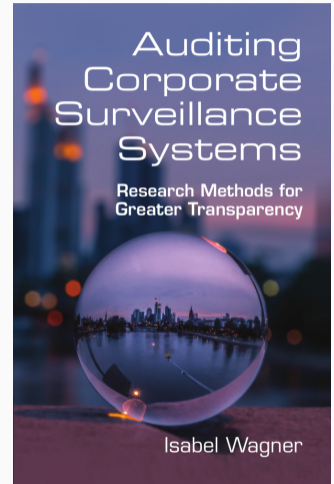
COURSE OVERVIEW

1. Introduction to corporate surveillance
2. How does corporate surveillance work?
3. How can we study corporate surveillance? Overview of methods and results for the example of stateful tracking
4. Experiment design
5. Data collection
6. Data analysis
7. Results from transparency research: Tracking, profiling, analytics, advertising
8. Results – Web services
9. Results – Mobile services
10. Results – Internet of Things
11. Countermeasures and their effectiveness
12. Towards real-world impact
13. Challenges & open issues

ABOUT THIS SLIDE DECK

- These slides are designed to accompany a lecture based on the textbook “Auditing Corporate Surveillance Systems: Research Methods for Greater Transparency” by Isabel Wagner, published in 2022 by Cambridge University Press.
- Except where otherwise noted (e.g., logos and cited works) this slide deck is Copyright © 2017-2022 Isabel Wagner
- The slides are free to use for non-commercial purposes, provided that the source of the slides, i.e. the textbook and its companion website, are cited appropriately
- Please leave this slide intact, but indicate modifications below.
 - Version 2022-04
 - Improved version for release on book website (Isabel Wagner)
- Updated versions of the original slide deck are available online: corporatesurveillance.org

Title	Auditing Corporate Surveillance Systems: Research Methods for Greater Transparency
Author	Isabel Wagner
Publisher	Cambridge University Press
Date	March 2022
Format	Hardback
ISBN-13	9781108837668
Website	corporatesurveillance.org



Book design ©2022 by Cambridge University Press

INTRODUCTION TO CORPORATE SURVEILLANCE

WHAT IS CORPORATE SURVEILLANCE?

- “Big Tech” corporations collect data about users
- Use this data for their profit
- But are not transparent about the details:
 - What data is collected?
 - Who is it shared with?
 - How is the data used, e.g. personalization, marketing, algorithmic decision-making, sale?
- Surveillance capitalism¹
 - New form of information capitalism focused on extracting data from users and social life
 - Aimed at behavior prediction and modification (“maximize engagement”)

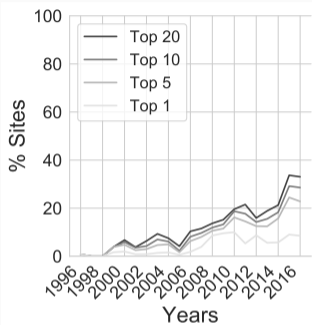
¹S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, 1 edition. New York: PublicAffairs, Jan. 2019.

CORPORATE SURVEILLANCE LANDSCAPE

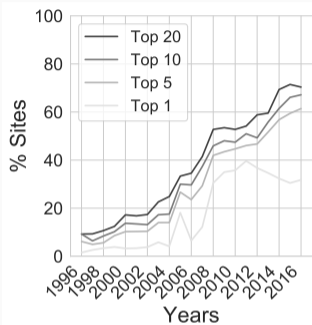
EVOLUTION OF CORPORATE SURVEILLANCE

- Following Google's history
- 1998: use *collateral data* to improve search results
 - E.g., search terms, spelling, dwell times, click patterns
- 2000: advertising matches ad keywords to search terms
- 2003: advertising matches ads to individuals
 - Collateral data used to create user profiles with demographics and interests
- Augment user profiles with data from sites other than Google
 - Users can be tracked by Google on sites that embed Google content
- Optimize ad placement
 - Instead of placing highest-paying ad first, rank ads by probability that an individual will click on them

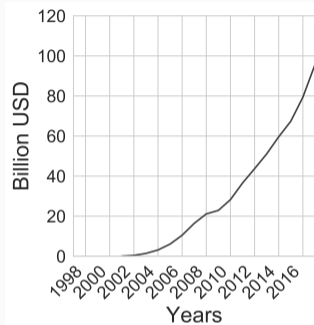
EVOLUTION OF CORPORATE SURVEILLANCE



Percentage of websites reached by the top trackers²



Percentage of websites reached by the top third parties



Google's advertising revenue in billion USD³

²A. Lerner, A. K. Simpson, T. Kohno, et al., "Internet Jones and the Raiders of the Lost Trackers: An Archaeological Study of Web Tracking from 1996 to 2016," in *25th USENIX Security Symposium (USENIX Security 16)*, Austin, TX, USA: USENIX, 2016

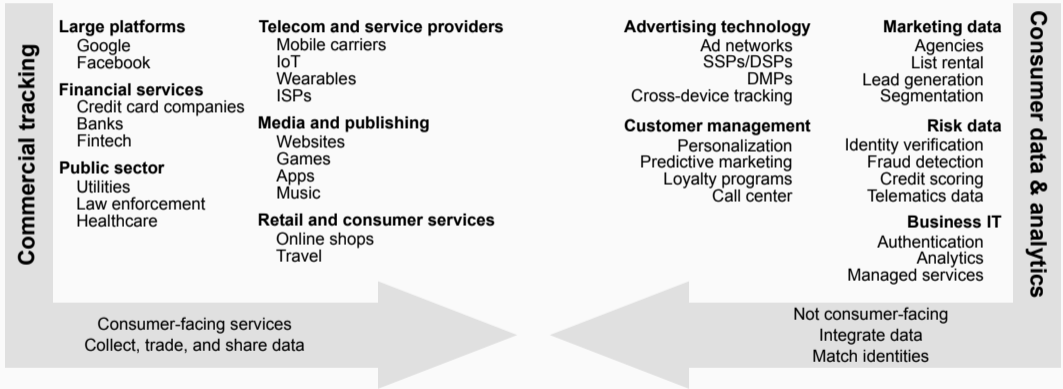
³J. Clement, *Google: Ad revenue 2001-2018*, <https://www.statista.com/statistics/266249/advertising-revenue-of-google/>, Feb. 2020

WHAT IS IN A “USER PROFILE”?

- From a 2020 BlueKai leak⁴
 - “a German man [...] used a prepaid debit card to place a €10 bet on an esports betting site on April 19. The record also contained the man’s address, phone number and email address.”
 - “one person, who lives in Istanbul, ordered \$899 worth of furniture online from a homeware store. We know because the record contained all of these details, including the buyer’s name, email address and the direct web address for the buyer’s order.”
 - “one person unsubscribed from an email newsletter run by an electronics consumer, sent to his iCloud address. The record showed that the person may have been interested in a specific model of car dash-cam. We can even tell based on his user agent that his iPhone was out of date and needed a software update.”

⁴Z. Whittaker, “Oracle’s BlueKai tracks you across the web. That data spilled online,” *TechCrunch*, Jun. 2020.

PLAYERS IN THE CORPORATE SURVEILLANCE ECOSYSTEM⁵



⁵W. Christl, "Corporate Surveillance in Everyday Life," Cracked Labs, Vienna, Austria, Tech. Rep., 2017, p. 93.

MOTIVES FOR CORPORATE SURVEILLANCE⁷

- Business intelligence
 - Improve service, tailor to users
- Economic motives: business models
 - Publishers: “free” web services paid for by advertising
 - Advertisers: save money by targeting only individuals who will buy their product
 - Large platforms: collect user profiles, then sell access to them (e.g., ability to target some individuals, without revealing information about the individuals)
 - “Surveillance is the business model of the Internet”⁶
- Optimization
 - For individuals: quantified self, health monitoring, smart homes
 - For societal processes: smart cities

⁶F. Y. Rashid, *Surveillance is the Business Model of the Internet: Bruce Schneier*, <https://www.securityweek.com/surveillance-business-model-internet-bruce-schneier>, Apr. 2014.

⁷N. Couldry, *The price of connection: 'surveillance capitalism'*, <http://theconversation.com/the-price-of-connection-surveillance-capitalism-64124>, Sep. 2016.

CORPORATE VS. GOVERNMENT SURVEILLANCE

- Surveillance
 - Not limited to CCTV-style video surveillance!
 - In the web, includes data about which websites we visit, where we click, how long we stay on a website, which topics we are interested in, etc.
 - The more we “live online”, the more we are subject to surveillance
- Government surveillance is out of scope
 - E.g., censorship, surveillance for “national security” and “intelligence”
 - Some aspects are similar to corporate surveillance: both are “black boxes”
- However:
 - NSA PRISM program: cooperation with tech corporations
 - All data collected as part of corporate surveillance may be available to government surveillance

UNDESIRABLE EFFECTS OF CORPORATE SURVEILLANCE

- “Saying you don’t care about privacy because you have nothing to hide is like saying you don’t care about free speech because you have nothing to say”⁸
- Privacy as prerequisite for other human rights: freedom of speech, freedom of thought, and freedom of assembly⁹
- Privacy needed for human autonomy and self-determination¹⁰
- Surveillance: creates pressure to conform, defines identities for users through user profiles
- Numerous big tech privacy promises & failures (Android location tracking, Google Nest microphones, Cambridge Analytica, etc.)

⁸E. Snowden, *Permanent Record*, 1st Edition. New York: Metropolitan Books, Sep. 2019.

⁹S. Wachter, “Privacy: Primus Inter Pares - Privacy as a Precondition for Self-Development, Personal Fulfilment and the Free Enjoyment of Fundamental Human Rights,” Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 2903514, Jan. 2017.

¹⁰Amnesty International, “Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights,” Amnesty International, London, UK, Tech. Rep. POL 30/1404/2019, 2019.

RIGHT TO EQUALITY AND NONDISCRIMINATION

- Facebook allowed discriminatory ad targeting:
 - Housing ads excluded certain ethnicities¹¹
 - Job ads targeted at certain age brackets¹²
 - Job ads targeted at certain genders¹³
- Lawsuits against Facebook (ACLU and others)
- Settled in March 2019: Facebook no longer allows targeting based on ethnicity, age, gender for job, finance, housing ads¹⁴

Facebook Lets Advertisers Exclude Users by Race

Facebook's system allows advertisers to exclude black, Hispanic, and other "ethnic affinities" from seeing ads.

by Julia Angwin and Terry Parris Jr., Oct. 28, 2016, 1 p.m. EDT

Facebook Job Ads Raise Concerns About Age Discrimination

Facebook Halts Ad Targeting Cited in Bias Complaints

¹¹J. Angwin and T. J. Parris, "Facebook Lets Advertisers Exclude Users by Race," *ProPublica*, Oct. 2016

¹²J. Angwin, N. Scheiber, and A. Tobin, "Facebook Job Ads Raise Concerns About Age Discrimination," *The New York Times*, Jan. 2018

¹³N. Scheiber, "Facebook Accused of Allowing Bias Against Women in Job Ads," *The New York Times*, Mar. 2019

¹⁴N. Scheiber and M. Isaac, "Facebook Halts Ad Targeting Cited in Bias Complaints," *The New York Times*, Mar. 2019

- Filter bubbles
 - Ranking of search results is important: results near the top receive most attention and clicks
 - Results personalized based on user's profile: create filter bubbles, reinforce user's existing views¹⁵
- Tampering with democratic processes
 - Biased search results can influence elections: undecided voters can be influenced by order of search results¹⁶
 - Cambridge Analytica: behavioral microtargeting based on prediction of Big5 personality profiles potentially influenced outcomes of 2016 US Presidential election and Brexit vote

¹⁵A. Hannak, P. Sapiezynski, A. Molavi Kakhki, et al., "Measuring Personalization of Web Search," in *Proceedings of the 22nd International Conference on World Wide Web*, ser. WWW '13, Rio de Janeiro, Brazil: ACM, 2013, pp. 527–538. doi: [10.1145/2488388.2488435](https://doi.org/10.1145/2488388.2488435).

¹⁶R. Epstein and R. E. Robertson, "The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections," *Proceedings of the National Academy of Sciences*, vol. 112, no. 33, E4512–E4521, Aug. 2015. doi: [10.1073/pnas.1419828112](https://doi.org/10.1073/pnas.1419828112).

- Human individuals have a right to privacy (e.g. Art. 12, Universal Declaration of Human Rights)
- Companies and organizations should be transparent so they are accountable to the public
- “Yet as individuals are made ever more transparent, corporate practices remain largely opaque.”¹⁷
- A reversal of what the right to privacy intends?!

¹⁷W. Christl, “Corporate Surveillance in Everyday Life,” Cracked Labs, Vienna, Austria, Tech. Rep., 2017, p. 93.

ARGUMENTS FOR MORE TRANSPARENCY

- Accountability for big tech
 - E.g., uncover unlawful business practices such as discriminatory ads
- Ensure functional democracy
 - E.g., uncover possibility of and evidence for voter manipulation
- Human autonomy and individuality¹⁸
 - E.g., uncover and debate big tech's experiments on non-consenting users, such as Facebook's emotional contagion experiments
- Audit effectiveness of and compliance with laws and regulations
 - E.g., new data protection regulations such as GDPR and CCPA
 - Evidence for the need of new laws and regulations

¹⁸Amnesty International, "Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights," Amnesty International, London, UK, Tech. Rep. POL 30/1404/2019, 2019.