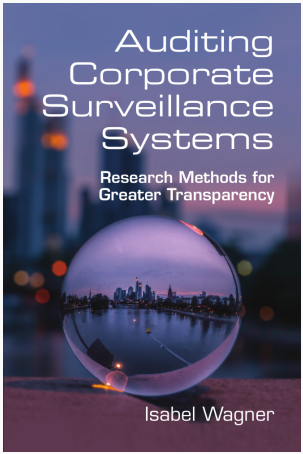
COUNTERMEASURES AND THEIR EFFECTIVENESS

Isabel Wagner

De Montfort University



OVERVIEW

- Ad blockers
  - How do they work?
  - How effective are they?
  - How prevalent are they?
  - Anti-Ad blockers
- Tracker blockers
- Fingerprinting blockers
- Obfuscation
- Tools for mobile applications

Ad blockers

How do ad blockers block?

- Network-based blocking
  - DNS blacklists (only domain/IP level, not fine-grained)
  - Interception proxies (fine-grained, but no HTTPS filtering)
- Browser-based blocking
  - Browser extensions, rely on API provided by browser (see Chrome 2018/19[1])
  - Requests are matched against filter list or against heuristics
  - Requests only sent to server if they are not blacklisted/whitelisted or if they pass the heuristic

[1] *https://blog.chromium.org/2018/10/trustworthy-chrome-extensions-by-default.html*

WHAT DO AD BLOCKERS BLOCK?

- Filter lists:
  - Different emphasis: ads, trackers, malware, etc.
  - Updated regularly, but maintained manually
  - Filter rules specified as regular expressions
  - Each outgoing requests is matched against all filter rules
  - Acceptable ads: mechanism in Adblock Plus to allow ads that are *visually* acceptable – no requirement to refrain from tracking
- Heuristics
  - Identify common third-party tracking techniques: identifying cookies, cookie sync, fingerprinting
  - Third-party hosts who have used these techniques on 3+ first-party sites are blocked

From Peter Lowe's DNS blacklist

```
127.0.0.1 101com.com
127.0.0.1 101order.com
127.0.0.1 123found.com
127.0.0.1 180hits.de
```

From EasyList

```
&act=ads_
&ad.vid=$~xmlhttprequest
,160x600;
,468x60-
&popunder=$popup
###A9AdsMiddleBoxTop
||007-gateway.com^$third-party
||0755.pics^$popup,third-party
||07zq44y2tmru.xyz^$popup
-api.adyoulike.com
-smartad.s3.amazonaws.com^
@@|blob:resource://$image
```

AD BLOCKING WITH MACHINE LEARNING[2]

- Disadvantages of filter lists: manual curation is time-consuming, time lag of many weeks possible, low coverage on low-ranking websites
- Machine learning: if model generalizes well, can reduce manual effort, time lag, and coverage issues
- Machine learning model:
  - Represent website as graph with HTML nodes, network nodes, script nodes, and parser nodes
  - Structural features (number of nodes/edges/siblings, node degrees, node attributes) and content features (request type, ad keywords, ad dimensions, query string parameters)
  - Training data: crawl top 10,000 websites, label requests as *ad* if it matches a public filter list
  - Random forest classifier achieves 95% accuracy and 86% recall

[2] U. Iqbal, P. Snyder, S. Zhu, *et al.*, "ADGRAPH: A Graph-Based Approach to Ad and Tracker Blocking," in *IEEE Symposium on Security & Privacy (S&P)*, San Francisco, CA, USA: IEEE, May 2020, pp. 65–78. DOI: *10.1109/SP.2020.00005*.

WHICH AD BLOCKERS ARE THERE?

Ad blocker	What	How
MVPS list	public blocklist	DNS blocking
Peter Lowe's list	public blocklist	DNS blocking
Privoxy	public default ruleset	interception proxy
Adblock Plus	public filter lists	browser extension
Disconnect	centralized filter list	browser extension
Ghostery	centralized filter list	browser extension
Privacy Badger	heuristics	browser extension
uBlock Origin	public filter lists	browser extension

EXPERIMENTAL DESIGNS FOR STUDYING AD BLOCKERS

Ad blockers	Websites	Performance measures
baseline, Adblock Plus, Disconnect, Ghostery, Privacy Badger, uBlock Origin, all combined	top 200,000 sites + two subsites each	third-party requests, reach
baseline, Adblock Plus, Ghostery, Do Not Track (each with default and max. protection)	top 500 sites + 500 from top 1 million	third-party requests, reach
baseline, Adblock Plus, Ghostery (each with max. protection, ad block only, privacy only)	top 1,000 sites	HTTP and HTTPS requests
Abine, Adversity, EasyList, EasyPrivacy, Ghostery, Fanboy list	top 500 sites	third-party requests, cookies
baseline, Ghostery, Abine TACO, Do Not Track	hand-selected, different topics	domains that set cookies

EFFECTIVENESS OF AD BLOCKERS

- Best adblockers block >80% of third-party requests
- But: reach of trackers only reduced to ~60%[3]
  - For example: combination of 5 ad blockers blocks 85% of third-party requests, but Google still reaches 60% of websites visited by the user
- Efficiency of ad blockers: system resources needed to perform the blocking
  - Browser vendors claim ad blocking harms system performance
  - Studies show: ad blocking improves browser performance, system performance, and user experience[4]

[3] G. Merzdovnik, M. Huber, D. Buhov, *et al.*, "Block Me If You Can: A Large-Scale Study of Tracker-Blocking Tools," in *2017 IEEE European Symposium on Security and Privacy (EuroS P)*, Paris, France: IEEE, Apr. 2017, pp. 319–333. DOI: *10.1109/EuroSP.2017.26*.

[4] K. Borgolte and N. Feamster, "Understanding the Performance Costs and Benefits of Privacy-focused Browser Extensions," in *Proceedings of The Web Conference 2020*, ser. WWW '20, Taipei, Taiwan: Association for Computing Machinery, Apr. 2020, pp. 2275–2286. DOI: *10.1145/3366423.3380292*.

EFFECTIVENESS OF FILTER LISTS

- How well does manual curation of filter lists work?[5]
  - EasyList: updates based on crowdsourced reports from EasyList forum
  - 30% of community effort for correcting false positives that break websites
  - Half of false positives persist for more than 1 month because they are not reported
- How do filter lists perform compared to heuristics?[6]
  - Heuristic based on invisible pixels: invisible pixels do not carry content, so invisible pixels are always trackers
  - Invisible pixels present on 94% of domains, represent more than 30% of third-party images
  - Disconnect list misses 30% of invisible pixel trackers, EasyList/EasyPrivacy misses 25%

[5] M. Alrizah, S. Zhu, X. Xing, *et al.*, "Errors, Misunderstandings, and Attacks: Analyzing the Crowdsourcing Process of Ad-blocking Systems," in *Proceedings of the Internet Measurement Conference*, ser. IMC '19, Amsterdam, Netherlands: Association for Computing Machinery, Oct. 2019, pp. 230–244. DOI: *10.1145/3355369.3355588*.

[6] I. Fouad, N. Bielova, A. Legout, *et al.*, "Missed by Filter Lists: Detecting Unknown Third-Party Trackers with Invisible Pixels," *Proceedings on Privacy Enhancing Technologies*, vol. 2020, no. 2, pp. 499–518, Apr. 2020. DOI: *10.2478/popets-2020-0038*.

PREVALENCE OF AD BLOCKERS

- Cannot evaluate with active measurement => need passive real traces
- Detecting ad block presence in traffic traces:
  - Requests for updated filter lists
  - Differences in percentage of ad requests (calibrated with active measurement: <5% ad requests indicate ad block usage)
- Residential broadband data, 2015[7]:
  - 22% likely to use Adblock Plus, another 15% with low ad request percentage
- comScore data, 2016[8]:
  - 17% in US+UK, 37% in Germany

[7] E. Pujol, O. Hohlfeld, and A. Feldmann, "Annoyed Users: Ads and Ad-Block Usage in the Wild," in *Proceedings of the 2015 Internet Measurement Conference*, ser. IMC '15, Tokyo, Japan: ACM, 2015, pp. 93–106. DOI: *10.1145/2815675.2815705*.

[8] M. Malloy, M. McNamara, A. Cahn, *et al.*, "Ad Blockers: Global Prevalence and Impact," in *Proceedings of the 2016 Internet Measurement Conference*, ser. IMC '16, Santa Monica, California, USA: ACM, 2016, pp. 119–125. DOI: *10.1145/2987443.2987460*.

ECONOMIC EFFECT OF AD BLOCKERS

- Mathematical model for ad revenue[9]
  - Base price for ad impressions (published figures)
  - Quality of publisher (Alexa rank)
  - User's purchasing intent (estimated using passive HTTP traces)
- 90% of ad revenue earned by top 5-10% of ad networks from top 35-55% of users
- If top 5% of users block ads: revenue could drop by 35-60%
- Hence, proposals for "acceptable ads"
- And...

[9] P. Gill, V. Erramilli, A. Chaintreau, *et al.*, "Follow the Money: Understanding Economics of Online Aggregation and Advertising," in *Proceedings of the 2013 Conference on Internet Measurement Conference*, ser. IMC '13, Barcelona, Spain: ACM, 2013, pp. 141–148. DOI: *10.1145/2504730.2504768*.

Anti-ad blockers

ANTI-AD BLOCKERS

- Circumventing ad blockers:
  - Keep changing domain names and HTML element identifiers
  - Exploit bugs, such as Chrome's WebSocket bug[10]
- Counter-blocking ad blockers: detect user of ad blocker and block user[11]
  - Bait advertising elements:
    - HTML elements named specifically to trigger ad blocker
    - Anti-adblock script then tries to access CSS properties of the element (e.g. width)
  - Bait scripts:
    - JS code that sets variable value or creates object
    - Anti-adblock script then checks for correct value or presence of object

[10] M. A. Bashir, S. Arshad, E. Kirda, *et al.*, "How Tracking Companies Circumvented Ad Blockers Using WebSockets," in *Proceedings of the Internet Measurement Conference 2018*, ser. IMC '18, Boston, MA, USA: ACM, 2018, pp. 471–477. DOI: *10.1145/3278532.3278573*.

[11] R. Nithyanand, S. Khattak, M. Javed, *et al.*, "Adblocking and Counter Blocking: A Slice of the Arms Race," in *6th USENIX Workshop on Free and Open Communications on the Internet (FOCI 16)*, Austin, TX, USA: USENIX, Aug. 2016.

PREVALENCE OF ANTI-AD BLOCKERS

- Detection of anti-ad block:
  - Presence of anti-ad block script, e.g. listed in Anti-Adblock Killer List
  - Visual changes to website

	Anti-ad block present	Visual changes to website
2016	6.7% of top 5k[12]	6 sites (0.12%)
2017	5% of top 100k[13]	0.7% of top 100k[14]
2018	30% of top 10k[15]	6.6% of top 10k

[12] R. Nithyanand, S. Khattak, M. Javed, *et al.*, "Adblocking and Counter Blocking: A Slice of the Arms Race," in *6th USENIX Workshop on Free and Open Communications on the Internet (FOCI 16)*, Austin, TX, USA: USENIX, Aug. 2016.

[13] 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*, ser. IMC '17, London, United Kingdom: ACM, 2017, pp. 171–183. DOI: *10.1145/3131365.3131387*.

[14] M. H. Mughees, Z. Qian, and Z. Shafiq, "Detecting Anti Ad-blockers in the Wild," *Proceedings on Privacy Enhancing Technologies*, vol. 2017, no. 3, pp. 130–146, Jul. 2017. DOI: *10.1515/popets-2017-0032*.

[15] S. Zhu, X. Hu, Z. Qian, *et al.*, "Measuring and Disrupting Anti-Adblockers Using Differential Execution Analysis," in *The Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, USA, Feb. 2018. DOI: *10.14722/ndss.2018.23331*.

ANTI-AD BLOCK FILTER RULES[16]

- Techniques for implementing anti-adblock filter rules:
  - Block anti-ad block script from loading
  - Exception rules that allow bait elements to load
  - Block visual elements that websites show after detecting ad blocker
- Community-created rulesets: EasyList, Anti-Adblock Killer List
  - Overlap of only 20% of domain names mentioned in rules
  - Long lag time: 90 days after anti-ad block added to website, EasyList covers 82% of cases, Anti-Adblock Killer List 32%

[16] 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*, ser. IMC '17, London, United Kingdom: ACM, 2017, pp. 171–183. DOI: 10.1145/3131365.3131387.

Tracker blockers

TRACKER BLOCKERS

- Broader in scope than ad blockers: block tracking in general, whether tracking is for advertising or not
- Techniques:[17]
  - Ad blocker
  - Replace social media buttons
  - Hide user's IP address
  - Strip tracking information from HTTP requests
  - Disable third-party cookies
  - Block execution of JavaScript
  - Do Not Track header

[17] T. Bujlow, V. Carela-Español, J. Solé-Pareta, *et al.*, "A Survey on Web Tracking: Mechanisms, Implications, and Defenses," *Proceedings of the IEEE*, vol. 105, no. 8, pp. 1476–1510, Aug. 2017. DOI: *10.1109/JPROC.2016.2637878*, F. Roesner, T. Kohno, and D. Wetherall, "Detecting and Defending Against Third-party Tracking on the Web," in *Proceedings of the 9th USENIX Conference on Networked Systems Design and Implementation*, ser. NSDI'12, San Jose, CA, USA: USENIX Association, 2012, pp. 12–12.

EFFECTIVENESS OF TRACKER BLOCKERS[18]

Tool	% requests to 3rd party	Reach of top tracker
No blocking	100	97
Adblock Plus	58	93
Disconnect	49	80
Ghostery	23	66
Privacy Badger	42	93
uBlock Origin	33	59
All tools combined	18	60
No blocking (mobile)	100	74
EasyList (mobile, proxy-based)	97	74
AdAway (mobile, DNS-based)	100	57
MOAB (mobile, DNS-based)	77	54

[18] G. Merzdovnik, M. Huber, D. Buhov, *et al.*, "Block Me If You Can: A Large-Scale Study of Tracker-Blocking Tools," in *2017 IEEE European Symposium on Security and Privacy (EuroS P)*, Paris, France: IEEE, Apr. 2017, pp. 319–333. DOI: *10.1109/EuroSP.2017.26*.

TRACKER BLOCKING WITH MACHINE LEARNING[19]

- Tracker blocking on mobile devices: may be infeasible to match against long filter lists
- Tracking on mobiles usually performed by third-party *tracking libraries*
- Machine learning to classify tracking requests
  - Training data: tracking requests originating from well-known tracking libraries
  - Features (plain-text traffic): full URL and HTTP headers, bag-of-words model
  - Features (TLS traffic): server name identification (SNI), DNS requests
  - Decision tree classifier achieves F1 scores of 95.5% (plain-text), 90.2% (TLS)
- Pre-trained decision trees take <1ms to evaluate on mobile devices

[19] A. Shuba and A. Markopoulou, "NoMoATS: Towards Automatic Detection of Mobile Tracking," *Proceedings on Privacy Enhancing Technologies*, vol. 2020, no. 2, pp. 45–66, Apr. 2020. DOI: *10.2478/popets-2020-0017*.

WEBSITE FUNCTIONALITY

- Aggressive blocking of trackers and ads can break website functionality
- Difficult to evaluate:
  - Breakage often affects user interactions -> hard to automate evaluation
  - Manual evaluation -> hard to ensure completeness, cannot evaluate large sample
- Existing studies: ~100 websites, 2–6 human evaluators[20]
- From browser vendor viewpoint: evaluate via increase in page reload rate over baseline level
  - Cliqz browser[21]: reload rate increased 10% (Adblock Plus), 25% (all potential trackers blocked)

[20] U. Iqbal, P. Snyder, S. Zhu, *et al.*, "ADGRAPH: A Graph-Based Approach to Ad and Tracker Blocking," in *IEEE Symposium on Security & Privacy (S&P)*, San Francisco, CA, USA: IEEE, May 2020, pp. 65–78. DOI: *10.1109/SP.2020.00005*, J. Mazel, R. Garnier, and K. Fukuda, "A comparison of web privacy protection techniques," *Computer Communications*, vol. 144, pp. 162–174, Aug. 2019. DOI: *10.1016/j.comcom.2019.04.005*.

[21] Z. Yu, S. Macbeth, K. Modi, *et al.*, "Tracking the Trackers," in *Proceedings of the 25th International Conference on World Wide Web*, ser. WWW '16, Montréal, Québec, Canada: International World Wide Web Conferences Steering Committee, Apr. 2016, pp. 121–132. DOI: *10.1145/2872427.2883028*.

Fingerprinting blockers

COUNTERMEASURES FOR FINGERPRINTING

- Blocking fingerprinting is harder than blocking stateful tracking: no on-device state that can be detected
- Randomize fingerprinting attributes
  - Server cannot link successive fingerprints to the same user
- Standardize fingerprinting attributes
  - Server cannot distinguish users if all have the same attribute values
  - Tor's anti-fingerprinting approach: make sure all Tor browsers have the same fingerprint[22]
    - 30+ distinct countermeasures
    - E.g, fixed window size, fixing keyboard event resolution, standard user-agent string, disabling HTML5 APIs that enable fingerprinting, etc.

[22] *https://2019.www.torproject.org/projects/torbrowser/design/*

FINGERPRINT RANDOMIZATION: PRIVARICATOR[23]

- Aim: make browser fingerprints unlinkable by randomizing them
  - Randomization must be consistent with real fingerprints
  - Randomization should not impact on user experience
- Randomization for screen properties (offsetWidth, offsetHeight, and getBoundingClientRect)
  - Random number between 0 and 100
  - Original number $\pm$5% noise
- Randomization for plugin enumeration
  - Probability to hide each entry
- Best randomization policies are effective against 3 state-of-the-art fingerprinters, change appearance of only 0.7% of top 1k sites

[23] N. Nikiforakis, W. Joosen, and B. Livshits, "PriVaricator: Deceiving Fingerprinters with Little White Lies," in *24th International Conference on World Wide Web (WWW)*, ser. WWW '15, Florence, Italy: ACM, 2015, pp. 820–830. DOI: *10.1145/2736277.2741090*.

OTHER FINGERPRINTING COUNTERMEASURES

- Motion sensor fingerprinting[24]
  - Sensor calibration: reduce manufacturing imperfections -> improve sensor readings AND reduce fingerprintability
  - Obfuscation: add noise to sensor readings
  - Quantization: convert real-value sensor readings into step function
- Extension fingerprinting[25]
  - Client-side diversification: alter/add fingerprintable attributes to browser extensions
- WebGL fingerprinting[26]
  - Standardize floating point operations

[24] A. Das, N. Borisov, and E. Chou, "Every Move You Make: Exploring Practical Issues in Smartphone Motion Sensor Fingerprinting and Countermeasures," *Proceedings on Privacy Enhancing Technologies*, vol. 2018, no. 1, pp. 88–108, Jan. 2018. DOI: *10.1515/popets-2018-0005*.

[25] E. Trickel, O. Starov, A. Kapravelos, *et al.*, "Everyone is Different: Client-side Diversification for Defending Against Extension Fingerprinting," in *28th USENIX Security Symposium (USENIX Security 19)*, Santa Clara, CA, USA: USENIX, Aug. 2019, pp. 1679–1696.

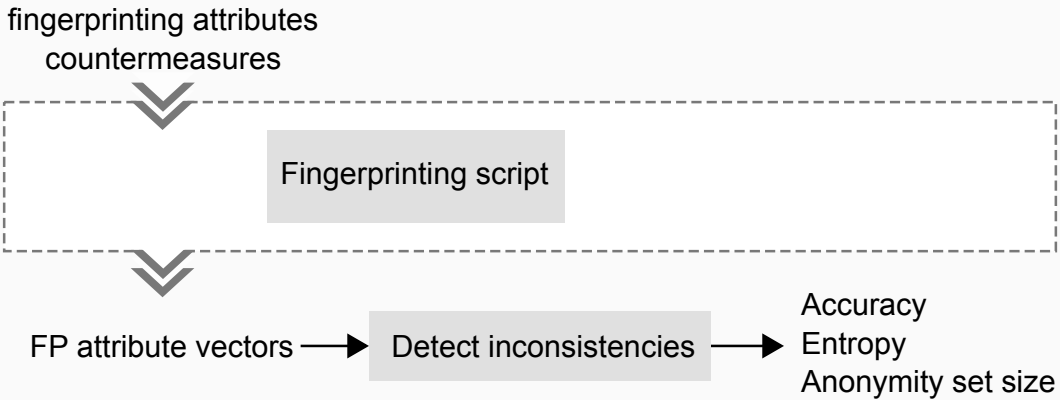
[26] S. Wu, S. Li, Y. Cao, *et al.*, "Rendered Private: Making GLSL Execution Uniform to Prevent WebGL-based Browser Fingerprinting," in *28th USENIX Security Symposium (USENIX Security 19)*, Santa Clara, CA, USA: USENIX, Aug. 2019, pp. 1645–1660.

ANTI-FINGERPRINTING BLOCKERS

- Fingerprinting countermeasures can introduce inconsistencies
  - Fingerprinters can detect presence of countermeasures
  - Sometimes even reconstruct original values of fingerprinting attributes
- Sources of inconsistencies for user-agent string, canvas, audio attributes:[27]
  - User-agent available through JS (navigator.userAgent) ↔ HTTP header (User-Agent)
  - User agent ↔ navigator.platform
  - Operating system ↔ WebGL renderer and vendor

[27] A. Vastel, P. Laperdrix, W. Rudametkin, *et al.*, "Fp-Scanner: The Privacy Implications of Browser Fingerprint Inconsistencies," in *27th USENIX Security Symposium (USENIX Security 18)*, Baltimore, MD, USA: USENIX, 2018, pp. 135–150.

DESIGN TO STUDY EFFECTIVENESS OF FINGERPRINTING BLOCKERS



EFFECTIVENESS OF FINGERPRINTING BLOCKERS

- Standardization of HTTP headers: percentage of uniquely identified browsers drops from 90% to 82% (desktop), 81% to 60% (mobile)
- Disabling JavaScript drops percentage to 29%[28]
- Percentage of unique browsers[29]
  - Most fingerprinting blockers: >50%
  - Brave browser: 7.2%
  - Tor browser: 1%
- Blocking of fingerprinting scripts by tracker blockers[30]
  - Disconnect: 25% of known canvas fingerprinting scripts
  - EasyPrivacy: 17.6%
  - WebRTC and AudioContext fingerprinting: even lower rates

[28] P. Laperdrix, W. Rudametkin, and B. Baudry, "Beauty and the Beast: Diverting Modern Web Browsers to Build Unique Browser Fingerprints," in *2016 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA: IEEE, May 2016, pp. 878–894. DOI: *10.1109/SP.2016.57*.

[29] A. Datta, J. Lu, and M. C. Tschantz, "Evaluating Anti-Fingerprinting Privacy Enhancing Technologies," in *The World Wide Web Conference*, ser. WWW '19, San Francisco, CA, USA: ACM, 2019, pp. 351–362. DOI: *10.1145/3308558.3313703*.

[30] 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*, ser. CCS '16, Vienna, Austria: ACM, 2016, pp. 1388–1401. DOI: *10.1145/2976749.2978313*.

Obfuscation

OBFUSCATION USING DUMMY TRAFFIC

- Aim: insert noise into the system to subvert corporate surveillance
- Dummy traffic to counter profiling[31]
  - Insert dummy HTTP requests that change the user's BlueKai profile
  - 5% dummy requests reduce similarity between original and obfuscated profile from 0.73 to 0.53
- Dummy traffic to hide search terms (TrackMeNot)[32]
  - Send dummy search queries so search engine cannot learn true user interests
  - Need to select realistic query topics (RSS) and match frequency and timing of real queries

[31] 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*, ser. WPES'18, Toronto, Canada: ACM, 2018, pp. 1–13. DOI: *10.1145/3267323.3268955*.

[32] V. Toubiana, L. Subramanian, and H. Nissenbaum, "TrackMeNot: Enhancing the privacy of Web Search," *arXiv:1109.4677 [cs]*, Sep. 2011. arXiv: *1109.4677 [cs]*.

OBFUSCATION: ADNAUSEAM[33]

- Aim: resistance to tracking through protest, by disrupting corporate surveillance business model
- Browser extension hides ads from user and blocks ad cookies, but clicks on percentage of ads in the background
  - Pollute profiles held by advertisers
  - Publishers have to pay for decoy ad clicks
- Ethical justification
  - Laudable aim? Yes, because corporate surveillance violates tenets of liberal democracy
  - Alternatives with lesser cost? Regulations (too slow), bandwidth negligible)

[33] D. C. Howe and H. Nissenbaum, "Engineering Privacy and Protest: A Case Study of AdNauseam," in *Proceedings of the 3rd International Workshop on Privacy Engineering*, vol. 1873, San Jose, CA, USA: IEEE, 2017, pp. 57–64.

Tools for mobile applications

TOOLS FOR MOBILE APPLICATIONS

- Blocking permission requests
  - DroidNet[34] (Android): quarantine new permission requests, display expert recommendations to suggest safe permissions
  - But: requires modified Android framework
  - ProtectMyPrivacy[35] (iOS): quarantine access to sensitive information, users can substitute anonymized versions, display crowdsourced recommendations
- Blocking access to the list of installed apps
  - Important: no permission needed to query installed apps, knowledge of 4 apps uniquely idenifies 95% of users, apps can be sensitive (e.g., health)
  - HideMyApp[36]: create container app with generic name for each sensitive app
  - User-level virtualization to launch sensitive app -> app is not registered in the OS
  - But: sensitive apps need to be installed from alternative app store

[34] B. Rashidi, C. Fung, A. Nguyen, *et al.*, "Android User Privacy Preserving Through Crowdsourcing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 3, pp. 773–787, Mar. 2018. DOI: *10.1109/TIFS.2017.2767019*.

[35] Y. Agarwal and M. Hall, "ProtectMyPrivacy: Detecting and Mitigating Privacy Leaks on iOS Devices Using Crowdsourcing," in *Proceeding of the 11th Annual International Conference on Mobile Systems, Applications, and Services*, ser. MobiSys '13, Taipei, Taiwan: ACM, 2013, pp. 97–110. DOI:

Summary

SUMMARY: COUNTERMEASURES AND THEIR EFFECTIVENESS

- Ad blockers: most common and well-known countermeasure
- Tracker blockers: aggressive blocking may break websites
- Fingerprinting blockers: some countermeasures may make browsers more identifiable
- Obfuscation
- Tools for mobile devices

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.
-
-
- 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