

2016 International Workshop on Privacy Engineering – IWPE '16
Tools in support of privacy engineering methodologies



Tools for privacy communications

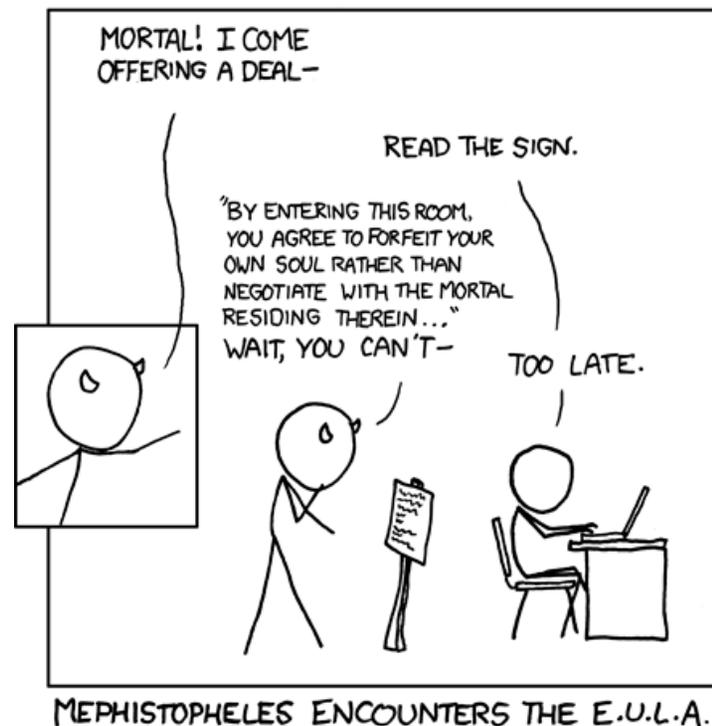
Aleecia M. McDonald, PhD
Non-resident Fellow, Stanford Center for Internet & Society

Privacy Communications, Part I



Privacy Polices

The big idea: reduce information asymmetries to support optimal privacy via self-regulation



Privacy Policies: Impractical

- To skim just first party privacy policies per year
 - 154 hours per person
 - 34 billion hours nationally
 - About the same as time spent surfing the web
- Value of time estimates
 - \$2,200 per person
 - \$492 billion nationally
 - More than spent on broadband connections

With L. F. Cranor. The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society* (2008).

Privacy Policies: Incomprehensible

- 9 basic questions, 6 policies
 - Mturk
 - Law & public policy grad students
 - Privacy Experts
- Within groups, Mturk and Expert agreement was moderate; student agreement substantial (Fleiss' Kappa statistical test)
- Mturk far off from the experts for financial data (40% median level of agreement with experts)
- Where policies were silent, experts interpret a practice is permitted; students say unclear
- If a policy claims a company “may” engage a practice, experts see it as permitted and students split

Reidenberg, Joel R., Breaux, T. D., Cranor, L. F., French, B., Grannis, A., Graves, J. T., Liu, F., McDonald, A. M., Norton, T. B., Ramanath, R., Russell, R. C., Sadeh, N., and Schaub, F. Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding. *Berkeley Technology Law Journal*, 30(1), May 2015, 39-88.

Blobs of Text Are Not Designed for Web-scale Tools

- Step 0: *find* the privacy policy
- Could do natural language processing...
- ...if humans could agree on gold standard truth!
- Hard to innovate for automated tools to help users navigate privacy policies
- So instead, we mess with the formats

Many Years Spent on Attempted Solutions

- Privacy policies as icons; “creative commons for privacy”
- Privacy policies as XML (P3P / compact P3P / Privacy Bird)
- Seals from TRUSTe and Better Business Bureau
- Layered policies
- Nutrition labels for privacy are great, but missing data

One problem: companies have no incentive to be clear

Mobile Policy Tools

privacy
choice



Can users ask questions or opt-out?

« Back

Next »

Summary

- You can ask privacy questions.
- You can ask privacy questions or opt-out of marketing.

[Customize summary](#)

Details

[review and edit details](#)

If you have any questions or concerns about our privacy policies, please contact us:
[CONTACT FORM URL] OR [EMAIL]
[PHYSICAL MAILING ADDRESS]

If you have given us contact information but do not want us to contact you with promotional or marketing information, you can opt-out here:

[LINK TO OPT-OUT FORM]

Please allow sufficient time for us to process your request.

B I

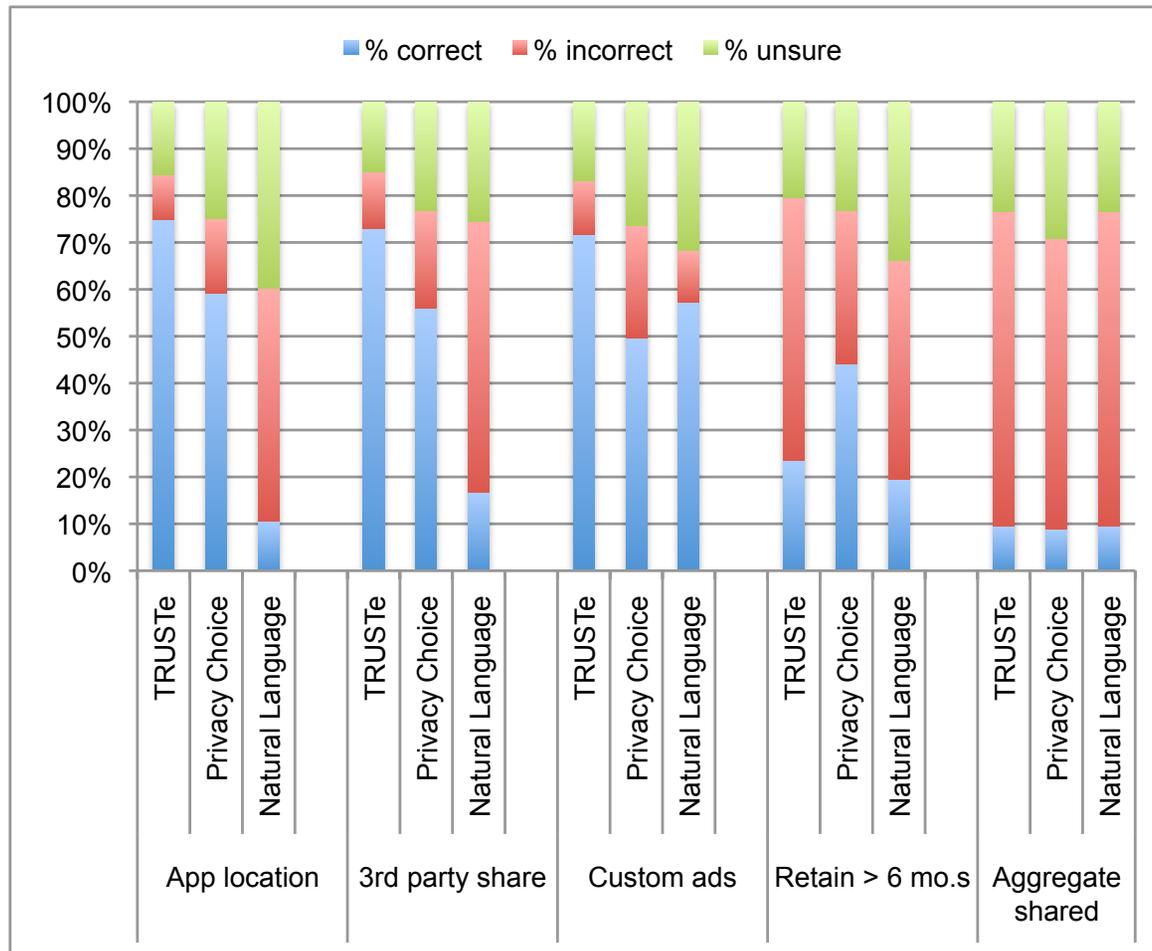
Tips

- Nearly all privacy policies offer a way for users to contact you with **privacy questions or concerns**, and this is a legal requirement in some jurisdictions.
- Option 1** applies if you **do not send marketing communications** by email, physical mail or otherwise.
- Option 2** applies if you send marketing communications and have an opt-out process on your website (this may be the same as the opt-out link inserted in your marketing emails)
- You must **insert your company contact information** (email address or a link to your contact form) into the Details section, as well

Is Geographic location collected?

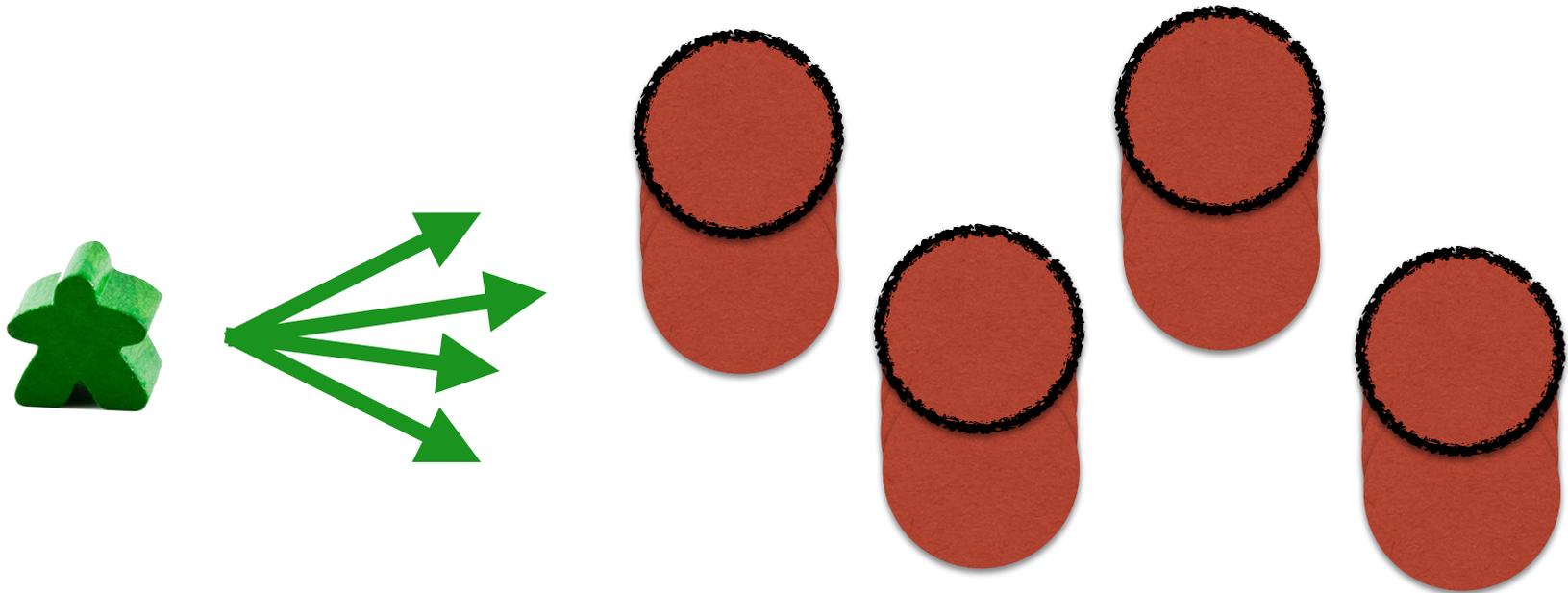
- Precise location from the device is collected
 - Provide location-based content ?
 - Check the user into a specific location for rewards, etc
 - Provide local search results
 - Provide local marketing offers
 - Provide geo-fencing services such as locating individuals or vehicles
 - Map travel or other locations of interest
 - Provide navigation, driving instructions
 - Enable sharing of location with friends, etc.
- User provides geographic location information
 - Provide location-based content ?
 - Provide local search results
 - Provide local marketing offers

Decent for Basics



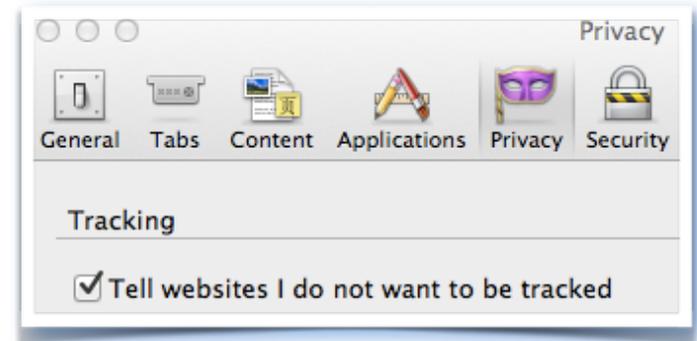
McDonald, A. M., and Lowenthal, T. Nano-Notice: Privacy Disclosure at a Mobile Scale. *Journal of Information Policy*, Vol. 3 (2013), pg. 331-354.

Privacy Communications, Part II



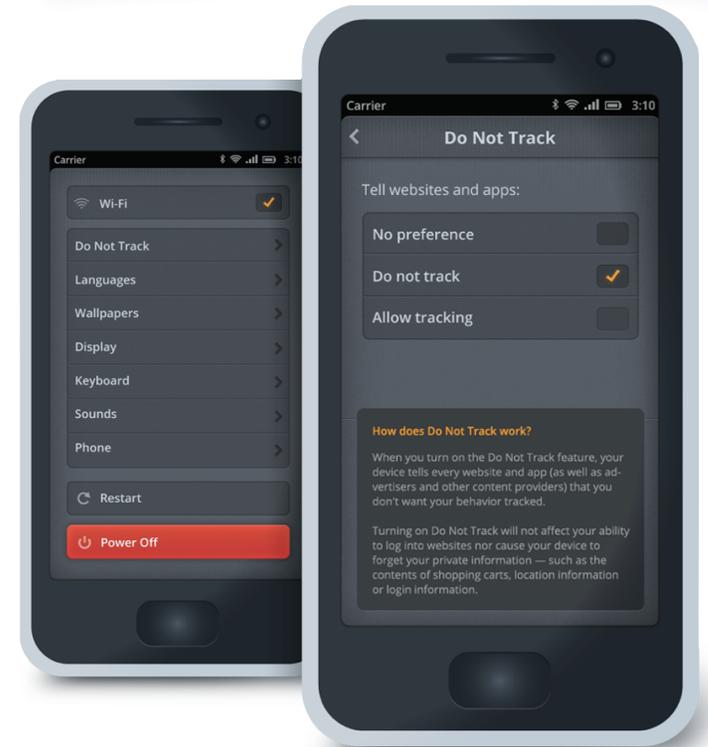
Do Not Track: A Polite Request for Privacy

All major browsers let users send a DNT request



Technically simple: HTTP header

Modest server-side implementation. Most user DNT requests just ignored.



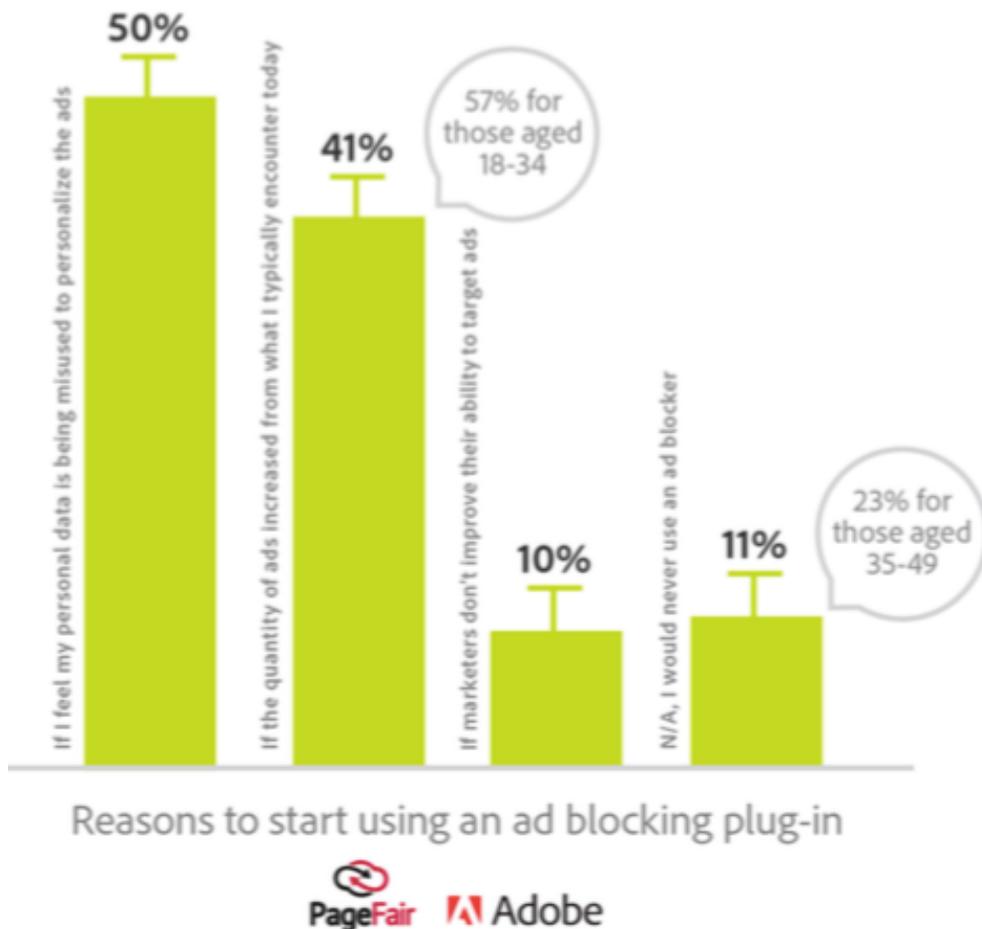
Do Not Track for EU?

Requirement	DAA Opt Out	W3C DNT	EFF DNT alone	EFF DNT & Privacy Badger Disconnect AdBlock
Consent by opt in?	No	Yes (varies by country)	No	Yes
Limits PII collection?	Maybe (varies by company)	Maybe (varies by company)	Yes	Yes
Consent before cookies set?	No	Yes	Yes	Yes
Can revoke?	Yes	Yes	Yes	Yes
Meets all 4	X	?	X	✓

Zuiderveen Borgesius, F. J., and McDonald, A. M. (2015). Do Not Track for Europe. *43rd Research Conference on Communication, Information and Internet Policy (Telecommunications Policy Research Conference)* September 26, 2015.

Ad Blockers: When “Please” Has Failed

- Most users are ok with ads for free content, not ads + data
(McDonald, A. M., and Cranor, L. F. Americans’ Attitudes About Internet Behavioral Advertising Practices. Proceedings of the 9th Workshop on Privacy in the Electronic Society (WPES) October 4, 2010.)

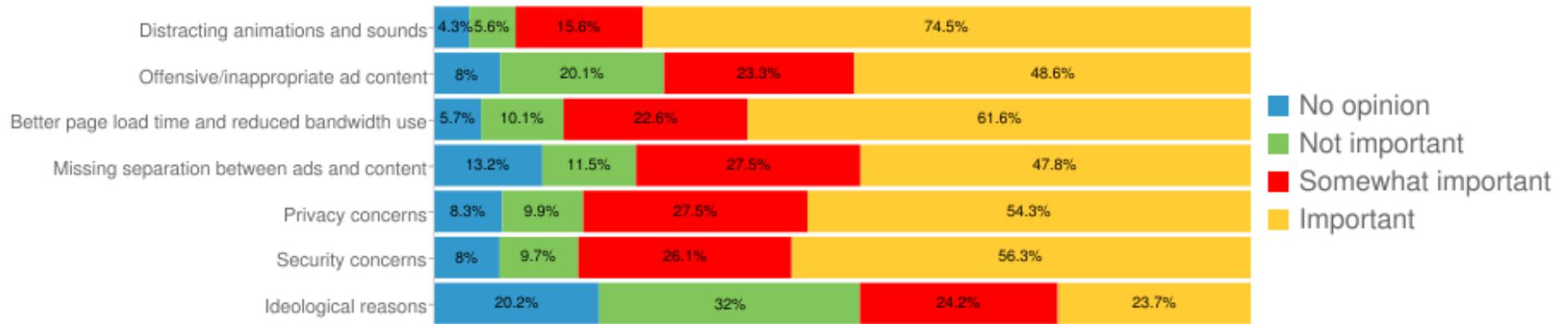


Of people *not* ad blocking, what would change their minds?

- 50% - personal data misused to personalize ads
- 41% - quality of ads increased
- 10% - marketers don't improve targeting
- 11% - N/A, would never install

Adobe and PageFair, The Cost of Ad Blocking (2015). <https://downloads.pagefair.com/wp-content/uploads/2016/05/2015_report-the_cost_of_ad_blocking.pdf>

Ad Blockers: When “Please” Has Failed



Of people who use AdBlock Plus, why? Important or somewhat important:

- 90% - distracting animations / sounds
- 84% - better page load time / reduced bandwidth
- 82% - security concerns
- 82% - privacy concerns
- 75% - missing separation between ads and content
- 72% - offensive / inappropriate ad content
- 48% - ideological reasons

Wladimir Palant, Adblock Plus user survey results [Part 2], November 7, 2011 <<https://adblockplus.org/blog/adblock-plus-user-survey-results-part-2>>

Wrap Up

- Consent underpins EU law, yet we have pretty poor privacy communications in both directions between companies and users
- We can do better!
 - Not intractable
 - Tools must be usable for engineers, and usable for users
 - Standards would help; role for regulators & laws