

Online Privacy: Industry Self-Regulation in Practice

Aleecia M. McDonald, PhD Candidate
Engineering & Public Policy



CyLab Usable Privacy and Security Laboratory
<http://cups.cs.cmu.edu/>

CarnegieMellon

Today's Google Tech Talk

- Background on industry self-regulation for online privacy

- CUPS research:
 1. The Cost of Reading Privacy Policies, *I/S* (with L. Cranor)

 2. A Comparative Study of Online Privacy Policies and Formats, *PETS* (with R. Reeder, P. Kelley, L. Cranor)

Papers available from **cups.cs.cmu.edu** or **aleecia.com/cv.html**

- Discussion of policy options



Fair Information Principles

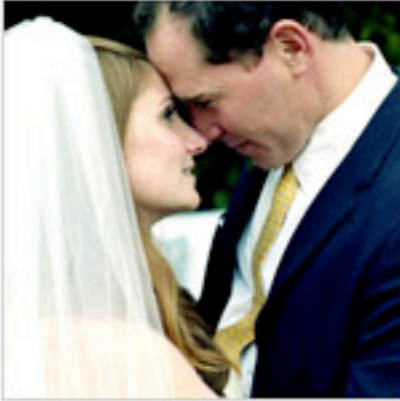
- Originated in the US in the 1970s
 - Concern about credit databases on main frames
 - Took hold internationally
- Provide a framework for approaching informational privacy
 - The FTC adopted 5 out of 8 FIPs (notice, choice, access, security, enforcement) in 1998
 - Online privacy policies are part of the FTC's response to the principle of "notice/awareness"



Online Privacy Policies


INSIDE NYTIMES.COM

STYLE »




Weddings & Celebrations

OPINION »



Op-Ed: Apollo Anniversary
Puzzles

MAGAZINE »




A Food Critic Comes to
Terms With His Appetite

OPINION »

Happy Days: Mad About It All


Readers consider the
roots and proper uses of
outrage.

N.Y. / REGION »




Seeking Room for New
Graves in Brooklyn

DANCE »



New Heights in Repertory

[Home](#) | [World](#) | [U.S.](#) | [N.Y. / Region](#) | [Business](#) | [Technology](#) | [Science](#) | [Health](#) | [Sports](#) | [Opinion](#) | [Arts](#) | [Style](#) | [Travel](#) | [Jobs](#) | [Real Estate](#) | [Automobiles](#) | [Back to Top](#)

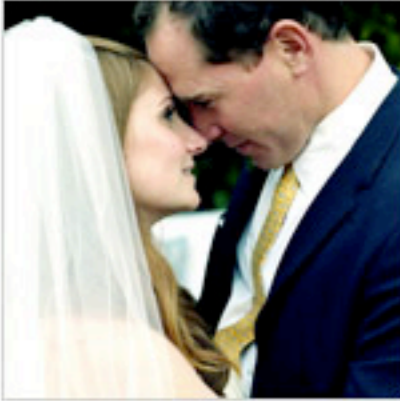
Copyright 2009 The New York Times Company | [Privacy Policy](#) | [Terms of Service](#) | [Search](#) | [Corrections](#) |  [RSS](#) | [First Look](#) | [Help](#) | [Contact Us](#) | [Work for Us](#) | [Site Map](#)



Online Privacy Policies


INSIDE NYTIMES.COM

STYLE »




Weddings & Celebrations

OPINION »



Op-Ed: Apollo Anniversary
Puzzles

MAGAZINE »




A Food Critic Comes to
Terms With His Appetite

OPINION »

Happy Days: Mad About It All


Readers consider the
roots and proper uses of
outrage.

N.Y. / REGION »



Seeking Room for New
Graves in Brooklyn

DANCE »



New Heights in Repertory

[Home](#) | [World](#) | [U.S.](#) | [N.Y. / Region](#) | [Business](#) | [Technology](#) | [Science](#) | [Health](#) | [Sports](#) | [Opinion](#) | [Arts](#) | [Style](#) | [Travel](#) | [Jobs](#) | [Real Estate](#) | [Automobiles](#) | [Back to Top](#)
[Copyright 2009 The New York Times Company](#) | [Privacy Policy](#) | [Terms of Service](#) | [Search](#) | [Corrections](#) | [RSS](#) | [First Look](#) | [Help](#) | [Contact Us](#) | [Work for Us](#) | [Site Map](#)



Online Privacy Policies

INSIDE NYTIMES.COM

STYLE » OPINION » MAGAZINE » OPINION » N.Y. / REGION » DANCE »

Weddings & Celebrations Op-Ed: Apollo Anniversary Puzzles A Food Critic Comes to Terms With His Appetite Happy Days: Mad About It All Readers consider the roots and proper uses of outrage. Seeking Room for New Graves in Brooklyn New Heights in Repertory

Home | World | U.S. | N.Y. / Region | Business | Technology | Science | Health | Sports | Opinion | Arts | Style | Travel | Jobs | Real Estate | Automobiles | Back to Top

Copyright 2009 The New York Times Company | **Privacy Policy** | Terms of Service | Search | Corrections | RSS | First Look | Help | Contact Us | Work for Us | Site Map

- Motivating problem: information asymmetry

- Leads to market failures

- FTC's solution: industry self-regulation with privacy policies

- Privacy policies:

- Often optional
- Content, appearance, structure up to the company
- Legally binding via deceptive practices or fraud actions

Industry Self Regulation in Theory

- Website owners voluntarily post online privacy policies
- FTC enforces policies via deceptive practices and fraud actions
- Consumers:
 - Read online privacy policies each time they visit new sites
 - Compare policies between sites
 - Buy from sites with the best privacy policies
- This creates a market place that efficiently rewards privacy protections



Industry Self Regulation in Practice

- Website owners voluntarily post online privacy policies
- FTC enforces policies via deceptive practices and fraud actions
- Consumers:
 - ~~Read online privacy policies each time they visit new sites~~
 - ~~Compare policies between sites~~
 - Buy from sites ~~with the best privacy policies~~
- ~~This creates a market place that efficiently rewards privacy protections~~



Value of Time to Read Privacy Policies



How Do We Engage People to Read Privacy Policies?

- Privacy community:
 - Build better privacy policies [Cranor, Hunton & Williams, etc.]
- Economics approach, create a national market [Laudon]
 - Perhaps no zone of negotiation for privacy markets [Garfinkel]
 - Perhaps inter-temporal discounting [Acquisti]
- **What would happen if people *did* read policies?**
 - How much time would that take?
 - How much would that time be worth?
- Put another way: what would happen if the FTC got what they asked for? Would industry self-regulation be viable in practice?



Estimating the Time to Read Privacy Policies

■ $T_R = p * R * n$

- p is the population of all Internet users
- R is the average time to read one policy
- n is the average number of unique sites Internet users visit annually

■ $p \approx 221$ million Americans online (Nielsen, May 2008)

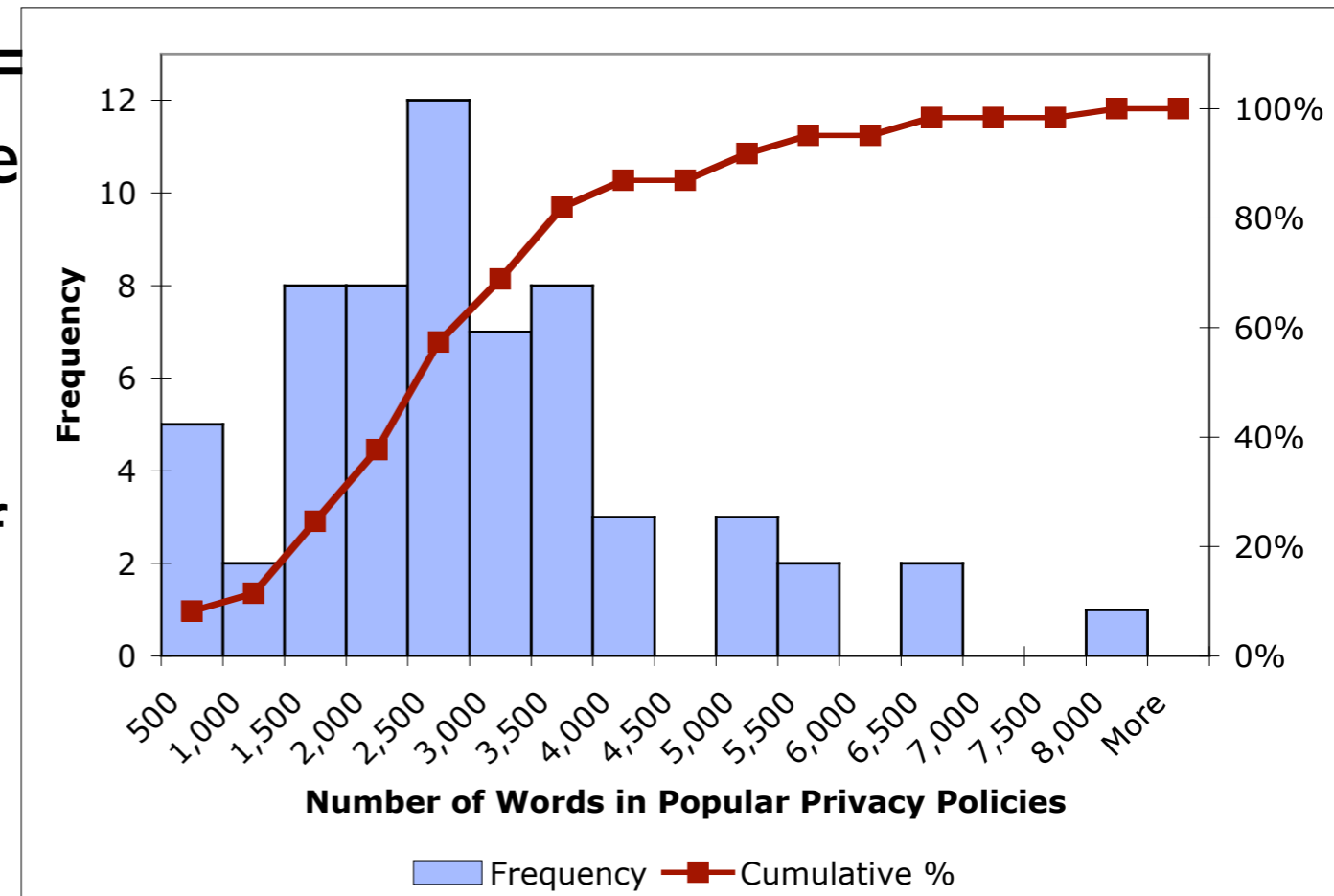


Estimating the Time to Read One Policy

■ $R = \text{avg time to read a policy} = \frac{\# \text{ words in policy}}{\text{reading rate}}$

■ To estimate words per policy:

- Measured the policy length of the 75 most visited websites
- Reflects policies people are most likely to visit

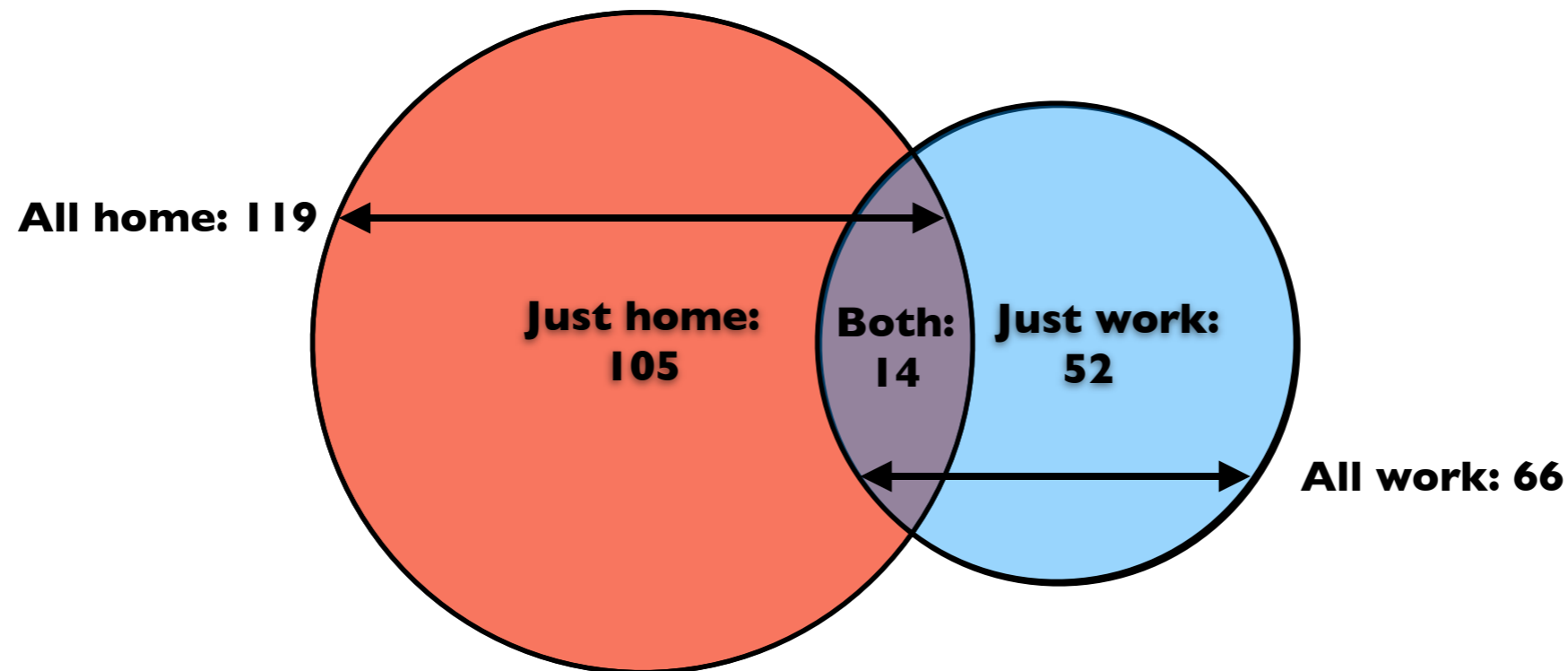


■ Reading rate \approx 250 WPM

- Low estimate: 2,071 words / 250 WPM = 8 minutes
- Mid estimate: 2,514 words / 250 WPM = 10 minutes
- High estimate: 3,112 words / 250 WPM = 12 minutes

Estimating the Average Number of Unique Sites (1 of 3)

- Nielsen estimates Americans visit 185 unique sites in a month:



- Overlap between websites viewed at work & home (e.g. Google)
- Time valued at a higher rate for home than work
- How do we allocate the 14 sites viewed at home and at work?

Estimating the Average Number of Unique Sites (2 of 3)

■ Lower bound monthly estimate:

- Assume all sites at work and home are first viewed at home
- Monthly estimate: 119 home, 52 work

■ Middle estimate:

- Assume half of overlap read at work, half at home
- Monthly estimate: 112 home, 59 work

■ Upper bound estimate:

- Assume all sites at work and home are first viewed at work
- Monthly estimate: 105 home, 66 work



Estimating the Average Number of Unique Sites (3 of 3)

- Looking for *annual* estimate – but cannot just multiply by 12
- Used a scale factor of 66% to 74%

Estimate	Scale factor	Policies read at work	Policies read at home	Total policies read
Lower	0.66	412 / year	942 / year	1354 / year
Middle	Weighted	467 / year	995 / year	1462 / year
High	0.74	586 / year	932 / year	1518 / year



Putting it All Together: Time to Read Online Policies

■ $T_R = p * R * n$

- $p \approx 221$ million Americans online (Nielsen, May 2008)
- $R \approx 10$ minutes per policy (lower estimate: 8; upper estimate: 12)
- n is the average number of unique sites an Internet user visits ≈ 1462 (lower estimate: 1354; upper estimate: 1518)

■ $R * n \approx 244$ hours per year per person (lower estimate: 181; upper estimate: 304)

■ $T_R \approx 53.8$ billion hours for all United States Internet users per year (lower estimate: 39.9 billion; upper estimate: 67.1 billion)



Is Reading Every Word the Right Model?

- How do people who read privacy policies use them in practice?
- More typical to look for specific information about concerns
- What if we imagine people skim for content rather than read each word?



Estimating the Time to Skim Privacy Policies

■ $T_s = p * S * n$

- p is the population of all Internet users
- S is the average time to skim one policy
- n is the average number of unique sites Internet users visit annually

■ S is the only input that changes; p and n are as before



Measuring the Time to Skim One Policy (1 of 2)

- Online study, $n = 212$
- Participants found answers to questions about privacy protections based on the text of a privacy policy
- Questions based on concerns people have about online privacy (Cranor et al, 2006)
- Asked five multiple-choice questions including “How can you remove yourself from Acme's email list?” and “Does the website use cookies?”
- Six policies of different lengths
 - One very short policy (928 words)
 - One very long (6,329)
 - Four close to 2,500 words
 - Median times from 18 to 26 minutes
- Problem: can manipulate the times based on the number of questions asked



Measuring the Time to Skim One Policy (2 of 2)

- Median times from warm up question ranged from four to eight minutes
 - Very conservative estimate
 - Averaged all six medians, first quartiles, third quartiles for estimates
- Low estimate: 3.6 minutes
- Middle estimate: 6.3 minutes
- High estimate: 11.6 minutes



Putting it All Together: Time to Skim Online Policies

■ $T_s = p * S * n$

- $p \approx 221$ million Americans online (Nielsen, May 2008)
- $S \approx 6.3$ minutes per policy (lower estimate: 3.6; upper estimate: 11.6)
- n is the average number of unique sites an Internet user visits as before: ≈ 1462 (lower estimate: 1354; upper estimate: 1518)

■ $p * S \approx 154$ hours per year per person (lower estimate: 81; upper estimate: 293)

■ $T_s \approx 33.9$ billion hours for all people per year (lower estimate: 17.9 billion, upper estimate: 64.8 billion)



Estimating the Value of Time

- Becker argued we should consider the value of time as an implicit cost of goods and services (Becker, 1965)
 - Opportunity cost of time is a major part of education cost
 - Cost to see a play includes the value audience members place on their own time
- Economics literature:
 - Time should be valued as salary plus overhead (Leunig, 2005)
 - In US, overhead is estimated as twice the rate of take home pay (Kmetovicz, 1992)
- Through revealed-preferences and willingness-to-pay studies, people value their leisure time at one quarter their take home pay (Leunig, 2005)



Value of Time by Location

- Where W is national average wages
 - Reading policies at work should be valued as $2W$
 - Reading policies at home should be valued as $\frac{1}{4}W$
- $W = \$17.93$ (BLS, March 2008)

Location	Average value of time
Work	\$ 35.86 / hour
Home	\$ 4.48 / hour



Conclusion Table

	Personal		National	
	Value to skim	Value to read	Value to skim	Value to read
Lower estimate	\$1,140	\$2,533	\$251.9 B	\$559.7 B
Middle estimate	\$2,226	\$3,534	\$492 B	\$781 B
Upper estimate	\$4,870	\$5,038	\$1.1 T	\$1.1 T



Discussion: Putting These Numbers in Perspective

- Time to read is greater than the time to handle spam, and on par with the current time websurfing
- Value of time to read or skim is several times greater than the cost of broadband access
- If companies cannot make privacy policies more useable, regulation improving disclosure may be insufficient
 - Saying more may improve transparency, but may also increase the costs to read



Discussion: Out of Balance?

- Many privacy concerns stem from advertisements
 - “It is unclear whether consumers even understand that their information is being collected, aggregated, and used to deliver advertising.” (FTC, 2008)
- Value of all online advertising in the US \approx \$21 billion in 2007 (IAB, 2008)
- Should Internet users give up \$492 billion of their time to protect themselves from a \$21 B industry?
 - Sales from direct mail are an order of magnitude higher than advertising costs (Petty, 2000)
- As envisioned, balance between costs borne by Internet users v. benefits of targeted ads for industry may misaligned

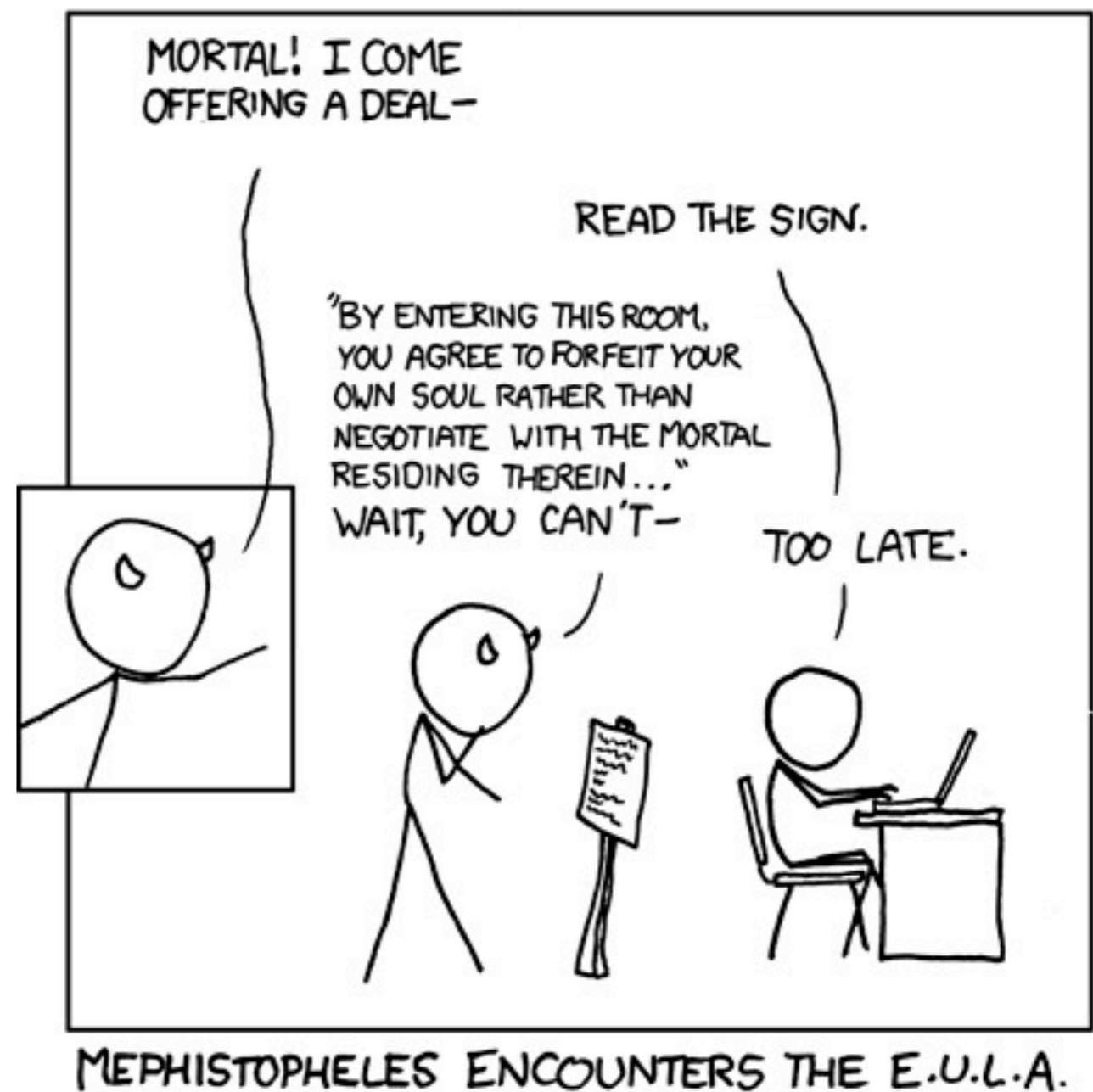


Standardized Privacy Policies



Do Privacy Policies Work?

- Conflict between legal liability for companies and the goal of notice
- College reading level *plus* jargon *plus* law
- Textual ambiguity, “weasel words” [Pollach]
- Each policy is different, must start from scratch
- Low readership [Jensen]
- Yet: people will pay a premium for privacy [Tsai]; FaceBook beacon backlash; they do care



Comic from xkcd.com

Can We Reduce Time Required to Read Policies Yet Improve Comprehension?

- One possibility: **standardized formats**
- Can highlight the most important information so people do not need to read the entire policy
- Users learn where to find information
- Easier to compare between policies



Do Standardized Policy Formats Help?

1. Natural Language
2. Layered
3. Privacy Finder



Acme Media Privacy Policy

Purpose and Scope

This policy discloses what information we gather about you when you visit any of our Web sites (all acme.com and Acme Network sites) or buy product directly from us. It describes how we use that information and how you can control it. Our privacy policy addresses:

[Information Acme gathers and tracks](#)

[Personal information](#)

[Aggregated tracking information](#)

[Cookies](#)

[Third Party Cookies](#)

[Third Party Advertising](#)

[Notification of Changes](#)

[How to update, correct, or delete your information](#)

Information Acme gathers and tracks

Acme collects two kinds of information about users: 1) data that users volunteer by signing up to receive news and product information, entering contests, completing surveys, or buying directly from us; and 2) aggregated tracking data we collect when users interact with us.

Personal information

We use the personal information you provide voluntarily to send information you've requested and to fulfill orders. The specific use of your personal information varies, depending on how you contact us:

- When you sign up online to receive Acme Network newsletters, Acme product and company news, and to participate in talkbacks on our sites you must provide your name, email address, and a password. We never sell or rent your email address or other personally identifiable information you provide us under these circumstances.
- When you register for an Acme conference, or sign up for a conference email list, we will send you email announcements and updates about Acme conferences. We send conference brochures to past conference attendees.

2.

Acme Privacy Summary

Scope

This policy discloses what information we gather about you when you visit any of our Web sites (all acme.com and Acme Network sites) or buy product directly from us. For more details, please refer to our [full privacy policy](#).

Personal Information

Acme collects two kinds of information about users:

1. data that users volunteer by signing up to receive news and product information, entering contests, completing surveys, or buying directly from us
2. aggregated tracking data we collect when users interact with us, such as access logs and web cookies

For more information about our information collection practices, please see our [full policy](#).

Uses

- We use the personal information you provide voluntarily to send information you've requested and to fulfill orders.
- When you sign up online to receive Acme Network newsletters, Acme product and company news, and to participate in talkbacks on our sites you must provide your name, email address, and a password. We never sell or rent your email address or other personally identifiable information you provide us under these circumstances.
- When you register for an Acme conference, or sign up for a conference email list, we will send you email announcements and updates about Acme conferences. We send conference brochures to past conference attendees.
- When you order books directly from us, or request book catalogs, we add you to our snailmail list, and we'll send you catalogs and other marketing pieces.
- When you enter a contest or sweepstakes, we may ask for your name, address, and email address so we can administer the contest and communicate with entrants about the results.

Acme Privacy Summary

Scope

This policy discloses what information we gather about you when you visit any of our Web sites (all acme.com and Acme Network sites) or buy product directly from us. For more details, please refer to our [full privacy policy](#).

Personal Information

Acme collects two kinds of information about users:

1. data that users volunteer by signing up to receive news and product information, entering contests, completing surveys, or buying directly from us
2. aggregated tracking data we collect when users interact with us, such as access logs and web cookies

For more information about our information collection practices, please see our [full policy](#).

Uses

- We use the personal information you provide voluntarily to send information you've requested and to fulfill orders.
- When you sign up online to receive Acme Network newsletters, Acme product and company news, and to participate in talkbacks on our sites you must provide your name, email address, and a password. We never sell or rent your email address or other personally identifiable information you provide us under these circumstances.
- When you register for an Acme conference, or sign up for a conference email list, we will send you email announcements and updates about Acme conferences. We send conference brochures to past conference attendees.
- When you order books directly from us, or request book catalogs, we add you to our snailmail list, and we'll send you catalogs and other marketing pieces.
- When you enter a contest or sweepstakes, we may ask for your name, address, and email address so we can administer the contest and communicate with entrants about the results.

Acme Media Privacy Policy

Purpose and Scope

This policy discloses what information we gather about you when you visit any of our Web sites (all acme.com and Acme Network sites) or buy product directly from us. It describes how we use that information and how you can control it. Our privacy policy addresses:

[Information Acme gathers and tracks](#)

[Personal information](#)

[Aggregated tracking information](#)

[Cookies](#)

[Third Party Cookies](#)

[Third Party Advertising](#)

[Notification of Changes](#)

[How to update, correct, or delete your information](#)

Information Acme gathers and tracks

Acme collects two kinds of information about users: 1) data that users volunteer by signing up to receive news and product information, entering contests, completing surveys, or buying directly from us; and 2) aggregated tracking data we collect when users interact with us.

Personal information

We use the personal information you provide voluntarily to send information you've requested and to fulfill orders. The specific use of your personal information varies, depending on how you contact us:

- When you sign up online to receive Acme Network newsletters, Acme product and company news, and to participate in talkbacks on our sites you must provide your name, email address, and a password. We never sell or rent your email address or other personally identifiable information you provide us under these circumstances.
- When you register for an Acme conference, or sign up for a conference email list, we will send you email announcements and updates about Acme conferences. We send conference brochures to past conference attendees.

Acme Incorporated Privacy Practices

[Opt-Out](#) | [Contact Site](#)

Acme Incorporated may share your information with:

- Companies that help this site fulfill your requests (for example, shipping a product to you), but these companies must not use your information for any other purpose
- Delivery companies that help this site fulfill your requests and who may also use your information in other ways
- Companies that are accountable to this site, though their privacy policies may be different from this site's
- People who may access your information from a public area, such as a bulletin board, chat room, or directory -- only if you request this

Privacy Policy Summary

Policy Statement 1 - Access log information

Our Web server collects access logs containing this information.

[Show data collection, use, and sharing details...](#)

This site may collect the following types of information about you:

- HTTP protocol information
- click-stream information

The ways your information may be used:

- For research and development, but without connecting any information to you
- To provide the service you requested
- To perform web site and system administration

With whom this site may share your information:

- Companies that help this site fulfill your requests (for example, shipping a product to you), but these companies must not use your information for any other purpose

Acme Incorporated Privacy Practices

[Opt-Out](#) | [Contact Site](#)

Acme Incorporated may share your information with:

- Companies that help this site fulfill your requests (for example, shipping a product to you), but these companies must not use your information for any other purpose
- Delivery companies that help this site fulfill your requests and who may also use your information in other ways
- Companies that are accountable to this site, though their privacy policies may be different from this site's
- People who may access your information from a public area, such as a bulletin board, chat room, or directory -- only if you request this

Privacy Policy Summary

Policy Statement 1 - Access log information

Our Web server collects access logs containing this information.

[Show data collection, use, and sharing details...](#)

This site may collect the following types of information about you:

- HTTP protocol information
- click-stream information

The ways your information may be used:

- For research and development, but without connecting any information to you
- To provide the service you requested
- To perform web site and system administration

With whom this site may share your information:

- Companies that help this site fulfill your requests (for example, shipping a product to you), but these companies must not use your information for any other purpose

Standardized Formats

	Layered	Privacy Finder
Big idea	One screen summary	Summary from P3P
Standardized	Headings; link to policy	Generated text; P3P itself
Flexibility	Text within headings	Text describing policies
Adoption	EU Article 29 guidance, several Fortune 500s	Available automatically for P3P via Privacy Finder
Development	Hunton & Williams law firm	AT&T first, now CUPS at Carnegie Mellon



Standardized Formats

	Layered	Privacy Finder
Big idea	One screen summary	Summary from P3P
Standardized	Headings; link to policy	Generated text; P3P itself
Flexibility	Text within headings	Text describing policies
Adoption	EU Article 29 guidance, several Fortune 500s	Available automatically for P3P via Privacy Finder
Development	Hunton & Williams law firm	AT&T first, now CUPS at Carnegie Mellon

Machine-readable XML representation of privacy policy statements



Standardized Formats

	Layered	Privacy Finder
Big idea	One screen summary	Summary from P3P
Standardized	Headings; link to policy	Generated text; P3P itself
Flexibility	Text within headings	Text describing policies
Adoption	EU Article 29 guidance, several Fortune 500s	Available automatically for P3P via Privacy Finder
Development	Hunton & Williams law firm	AT&T first, now CUPS at Carnegie Mellon

Machine-readable XML representation of privacy policy statements



Research Questions

- Do standardized formats help?
 - Accuracy
 - Time
 - Psychological acceptability
- How much variance is there between e-com privacy policies?
 - Selected six policies ranging from fairly readable to dreadful



Six Policies

■ Better

We share customer information only with affiliated companies and as described below:

- With third parties we retain to perform functions on our behalf, such as fulfilling orders, processing credit card payments, managing mailing lists, and delivering packages. These parties are restricted from using your information for any other purpose.
- We rent our snailmail list for one-time use to third parties we deem relevant and appropriate. We do not rent or sell our email lists.
- We release personal information when we believe that release is appropriate to comply with the law, or to protect the rights, property, or safety of Acme Incorporated, our users, or others. This may include exchanging information with other companies and organizations for fraud protection and credit risk reduction.



Six Policies

■ Better

We share customer information only with affiliated companies and as described below:

- With third parties we retain to perform functions on our behalf, such as fulfilling orders, processing credit card payments, managing mailing lists, and delivering packages. These parties are restricted from using your information for any other purpose.
- We rent our snailmail list for one-time use to third parties we deem relevant and appropriate. We do not rent or sell our email lists.
- We release personal information when we believe that release is appropriate to comply with the law, or to protect the rights, property, or safety of Acme Incorporated, our users, or others. This may include exchanging information with other companies and organizations for fraud protection and credit risk reduction.

■ Worse

Subject to your opt-out choices (see A4 below), The Acme Family of Companies may share your personal information with selected third parties so that they can send you promotional materials about goods and services (including special offers and promotions) offered by them. (We call this type of sharing "promotional sharing" or sharing for "promotional purposes.") When sharing your information for promotional purposes, The Acme Family of Companies attempts to select only reputable companies that offer high quality products and services. Moreover, The Acme Family of Companies will not share your e-mail address with third parties for promotional purposes, except when you consent to such sharing in the course of your participation in a Sponsored Activity as described below. When The Acme Family of Companies shares your personal information with a third party under any circumstance described in this "Third Parties



Six Policies

■ Better

We share customer information only with affiliated companies and as described below:

- With third parties we retain to perform functions on our behalf, such as fulfilling orders, processing credit card payments, managing mailing lists, and delivering packages. These parties are restricted from using your information for any other purpose.
- We rent our snailmail list for one-time use to third parties we deem relevant and appropriate. We do not rent or sell our email lists.
- We release personal information when we believe that release is appropriate to comply with the law, or to protect the rights, property, or safety of Acme Incorporated, our users, or others. This may include exchanging information with other companies and organizations for fraud protection and credit risk reduction.

■ Worse

Subject to your opt-out choices (see A4 below), The Acme Family of Companies may share your personal information with selected third parties so that they can send you promotional materials about goods and services (including special offers and promotions) offered by them. (We call this type of sharing "promotional sharing" or sharing for "promotional purposes.") When sharing your information for promotional purposes, The Acme Family of Companies attempts to select only reputable companies that offer high quality products and services. Moreover, The Acme Family of Companies will not share your e-mail address with third parties for promotional purposes, except when you consent to such sharing in the course of your participation in a Sponsored Activity as described below. When The Acme Family of Companies shares your personal information with a third party under any circumstance described in this "Third Parties



Six Policies

■ Better

We share customer information only with affiliated companies and as described below:

- With third parties we retain to perform functions on our behalf, such as fulfilling orders, processing credit card payments, managing mailing lists, and delivering packages. These parties are restricted from using your information for any other purpose.
- We rent our snailmail list for one-time use to third parties we deem relevant and appropriate. We do not rent or sell our email lists.
- We release personal information when we believe that release is appropriate to comply with the law, or to protect the rights, property, or safety of Acme Incorporated, our users, or others. This may include exchanging information with other companies and organizations for fraud protection and credit risk reduction.

■ Worse

Subject to your opt-out choices (see A4 below), The Acme Family of Companies may share your personal information with selected third parties so that they can send you promotional materials about goods and services (including special offers and promotions) offered by them. (We call this type of sharing "promotional sharing" or sharing for "promotional purposes.") When sharing your information for promotional purposes, The Acme Family of Companies attempts to select only reputable companies that offer high quality products and services. Moreover, The Acme Family of Companies will not share your e-mail address with third parties for promotional purposes, except when you consent to such sharing in the course of your participation in a Sponsored Activity as described below. When The Acme Family of Companies shares your personal information with a third party under any circumstance described in this "Third Parties



Readability

		NL Pages	Reading Ease	% Passive	# cross references	PF Words	NL Words
Worse	A	13	31.8	11%	27	880	6329
	B	7	35.5	22%	0	1964	3725
	C	6	36.3	17%	7	2011	2920
	D	8	42.8	18%	2	554	2586
	E	8	44.9	11%	0	1373	2550
Better	F	3	46.3	9%	1	1843	928



Readability

		NL Pages	Reading Ease	% Passive	# cross references	PF Words	NL Words
Worse	A	13	31.8	11%	27	880	6329
	B	7	35.5	22%	0	1964	3725
	C	6	36.3	17%	7	2011	2920
	D	8	42.8	18%	2	554	2586
	E	8	44.9	11%	0	1373	2550
Better	F	3	46.3	9%	1	1843	928

Flesch-Kinkaid Reading Ease

- 0-29: Very Confusing
- 30-49: Difficult
- 50-59: Fairly Difficult



Methods

- Between subjects design: one policy with a series of questions
- Tested questions, pilot tested online study, plus prior work
Reeder, R., Cranor, L., Kelley, P. and McDonald, A. *A User Study of the Expandable Grid Applied to P3P Privacy Policy Visualization*. (WPES 2008)
- August — December, 2008
- Recruited via blogs and craigslist for gift certificate drawing
- 15 conditions
- $n = 749$; 50 per condition
- Younger, well-educated, and confident with computers



Outliers

- Drawing meant some people just “click through”
 - Omitted participants who were clearly too fast
- People are sometimes interrupted
 - Omitted times that were clearly too slow



Comic from icanhascheezburger.com

Questionnaire Process

- Training question first, company's address: end of policy

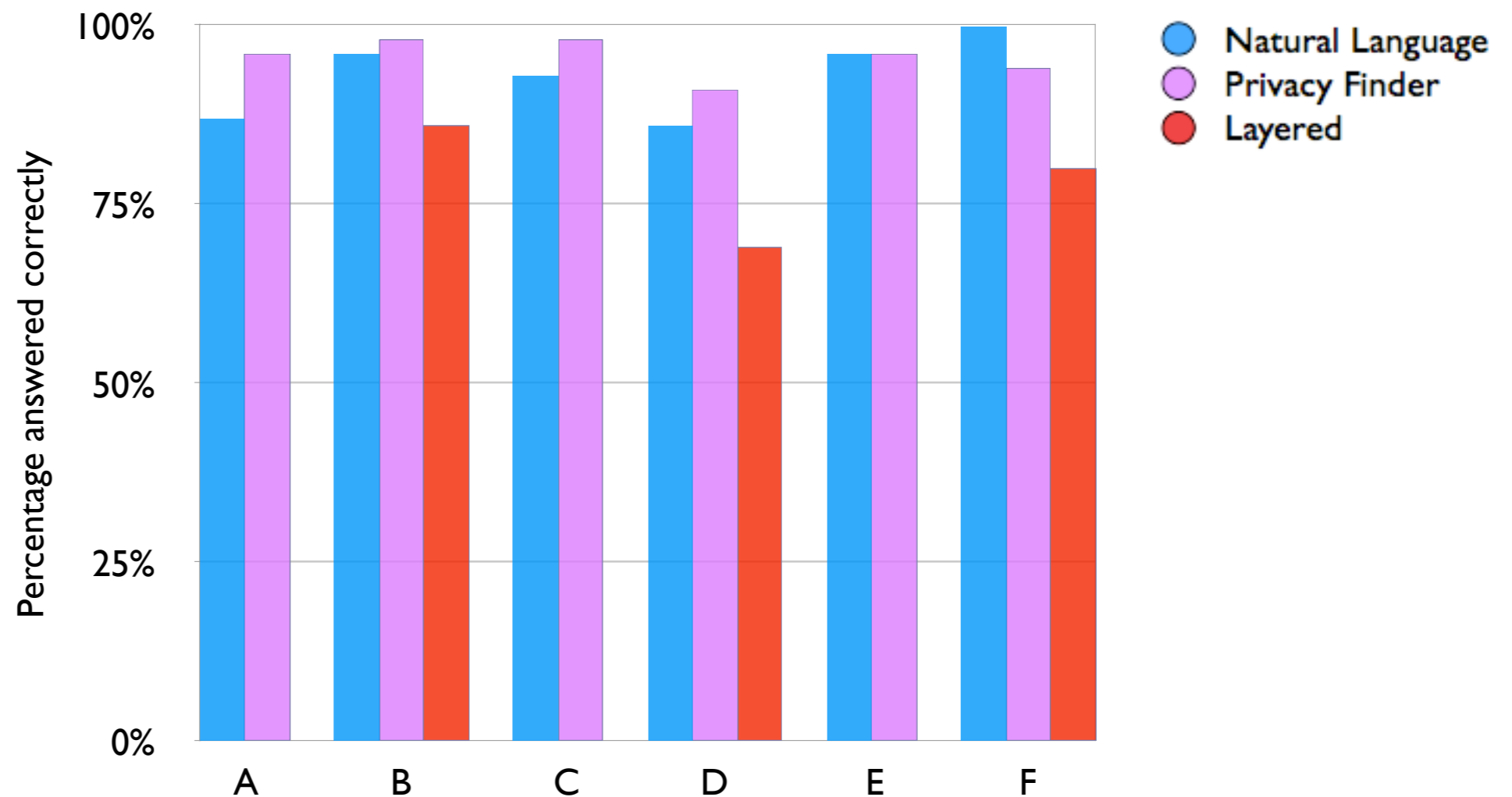
- Percentage correct answers for four random order questions:
 1. Does the Acme website use cookies?
 2. Does the company provide a link to a webform that allows you to remove yourself from Acme's email marketing list?
 3. Does this privacy policy allow Acme to share your email address with a company that might put you on their email marketing list (with or without your consent)?
 4. Does this privacy policy allow Acme to use your phone number for telemarketing?

- Also measured response times



...use cookies?

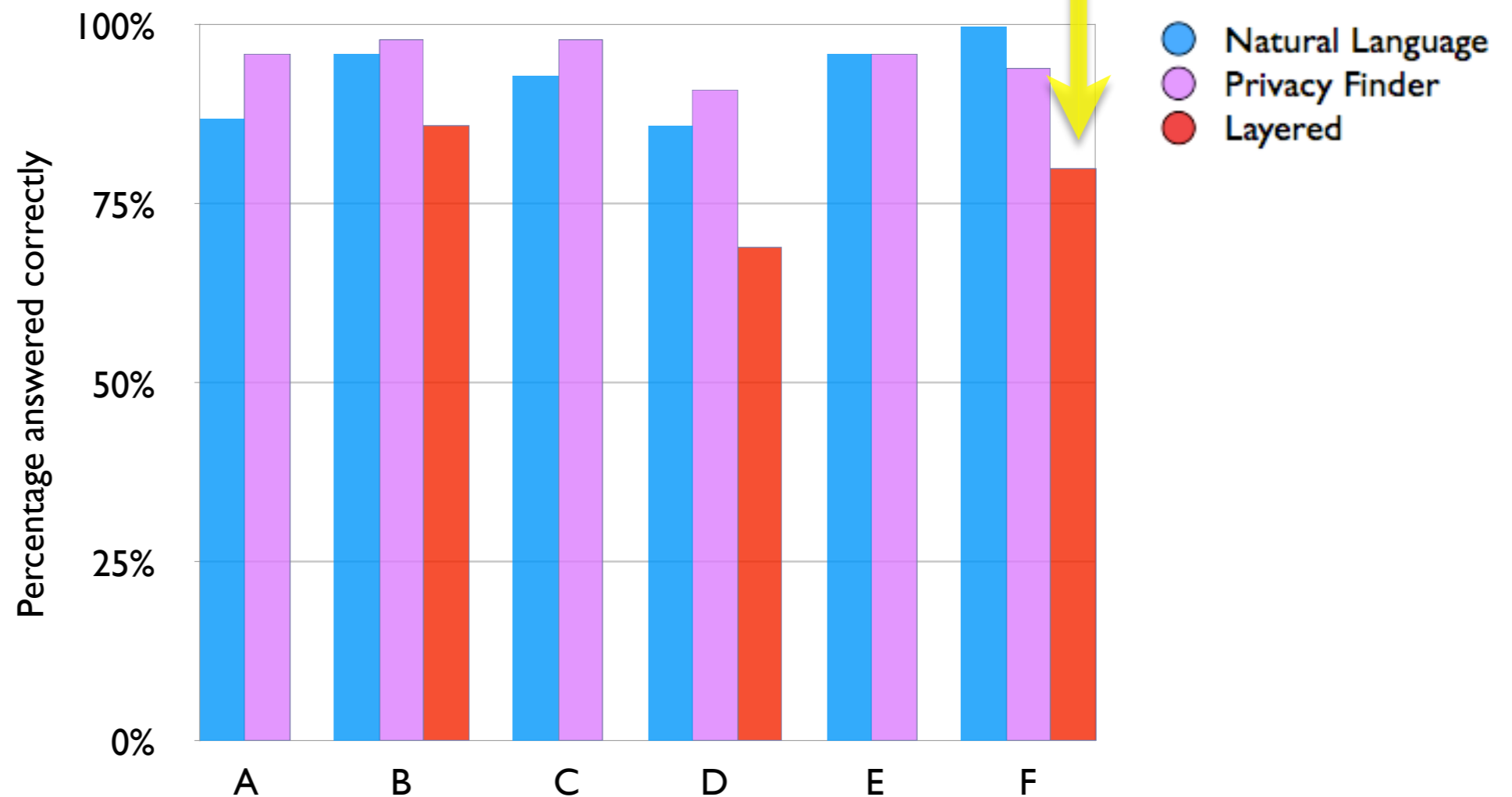
- High accuracy (91%)
- All policies mentioned cookies explicitly
- Layered worse (78%)



...use cookies?

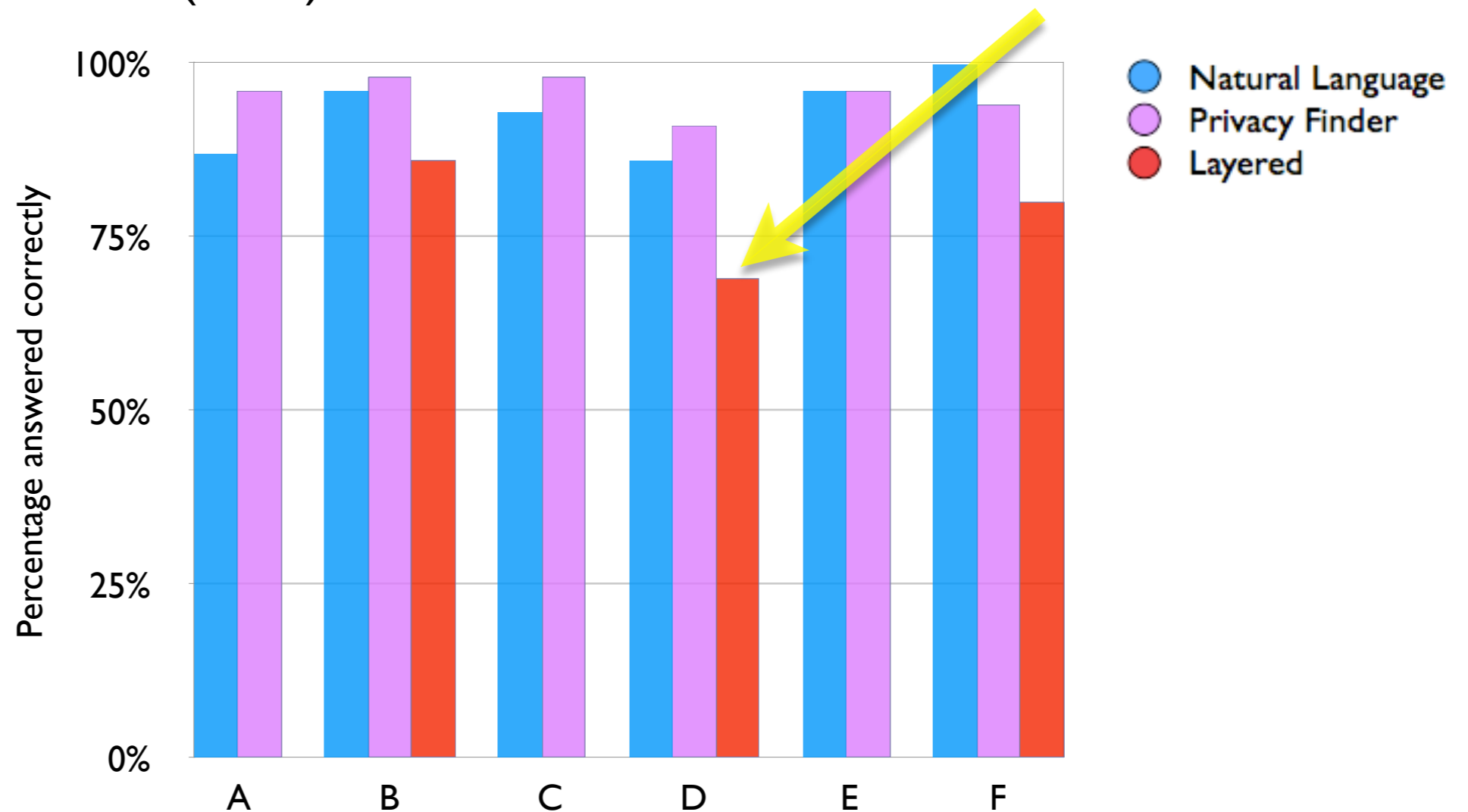
- High accuracy (91%)
- All policies mentioned cookies explicitly
- **Layered** worse (78%)

- F **Layered** (80%) under “Personal Information”



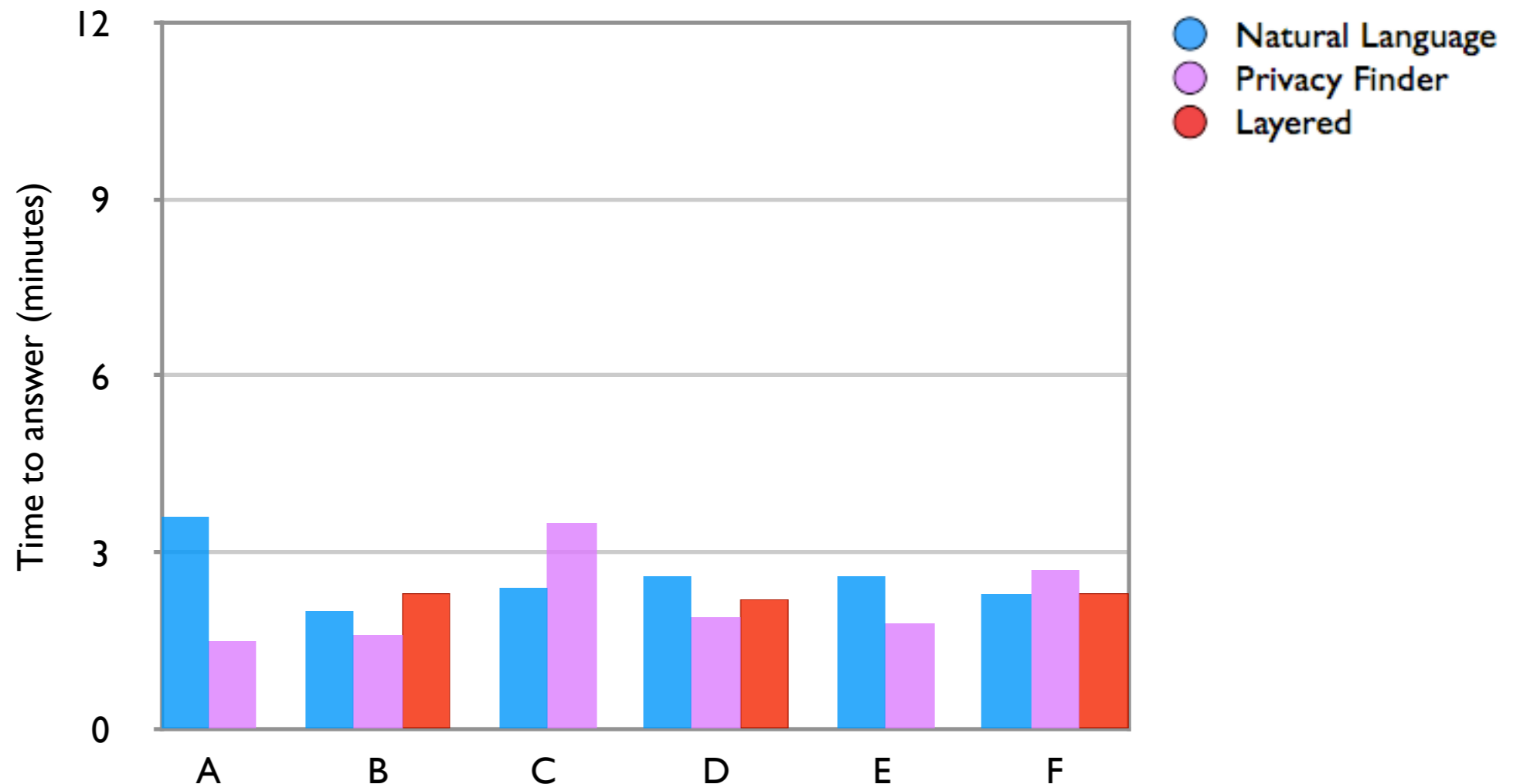
...use cookies?

- High accuracy (91%)
 - All policies mentioned cookies explicitly
 - **Layered** worse (78%)
- F **Layered** (80%) under “Personal Information”
 - D **Layered** (69%) “You may also turn off cookies in your browser”



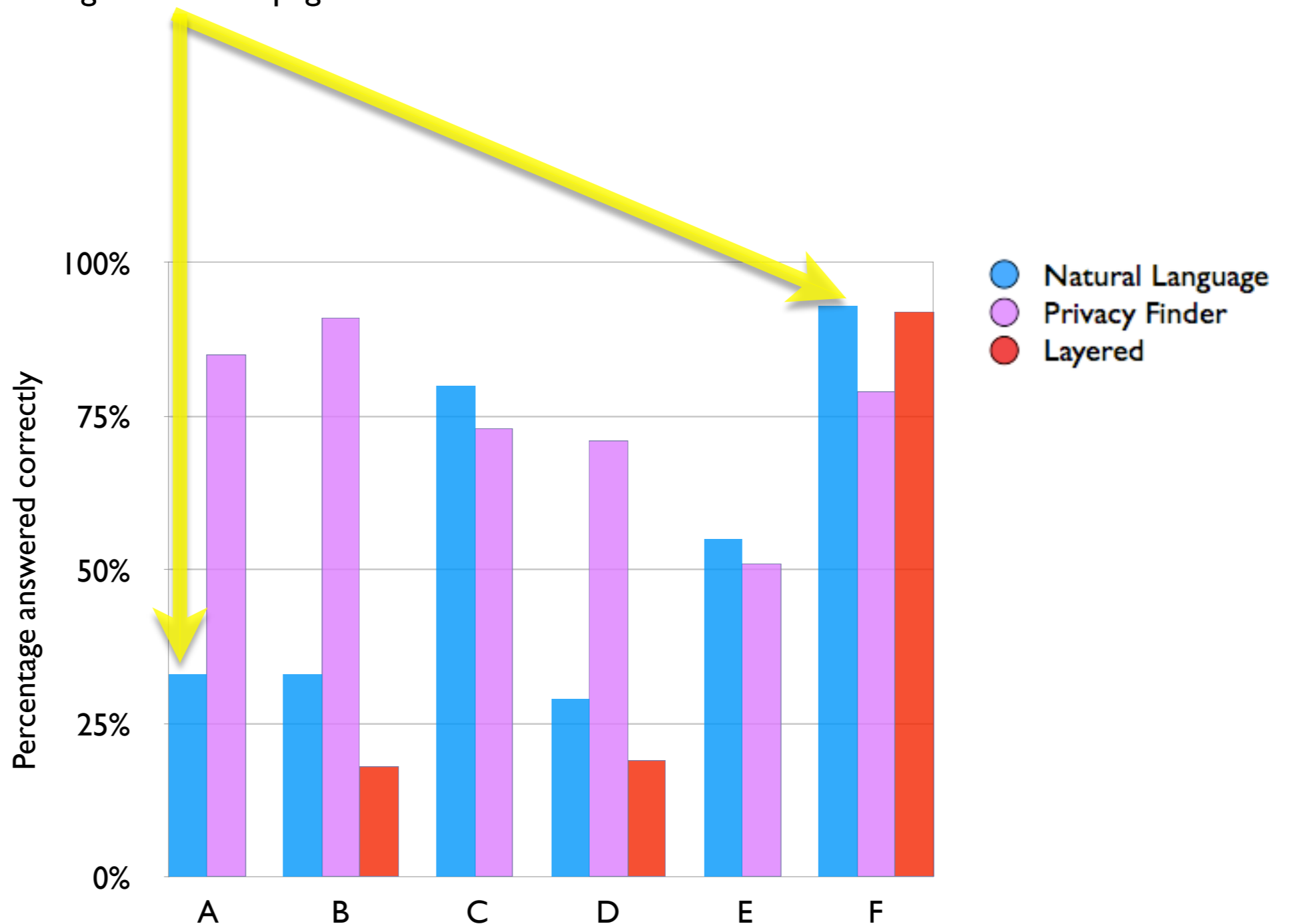
...use cookies?

- Shortest answer times (2.3 minutes)
- No significance for company, just format
- PF (2.1) & Layered (2.3) faster than NL (2.6)
- Layered → more incorrect answers



link to a webform... to remove yourself from Acme's email marketing list

- NL from 93% (F) to 33% (A)
- Required finding a link in 13 pages



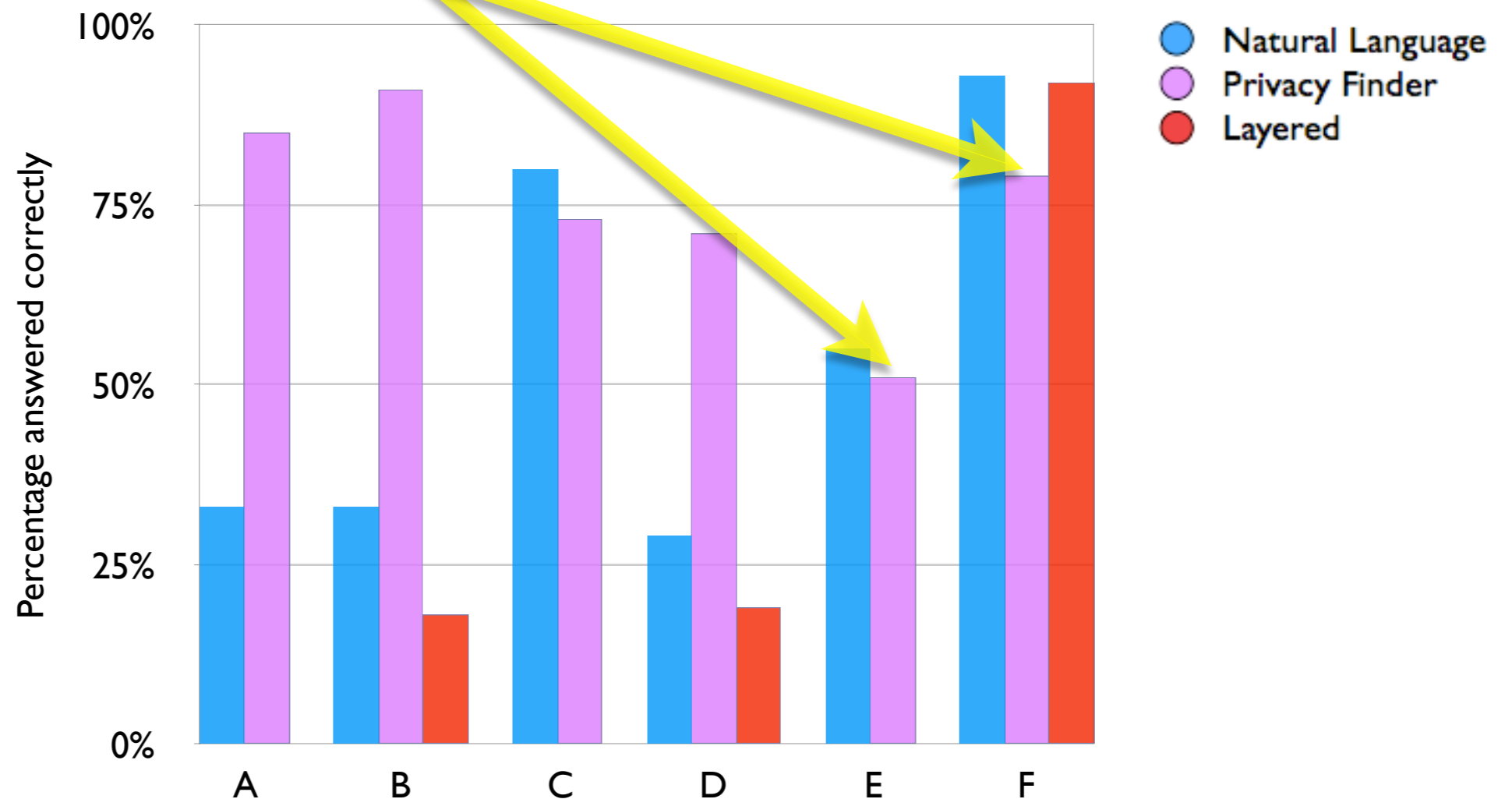
link to a webform... to remove yourself from Acme's email marketing list

- NL from 93% (F) to 33% (A)
 - Required finding a link in 13 pages
- PF from 91% (B) to 51% (E)



link to a webform... to remove yourself from Acme's email marketing list

- NL from 93% (F) to 33% (A)
 - Required finding a link in 13 pages
- PF from 91% (B) to 51% (E)
 - F PF (79%) same practices as E PF (51%), difference in free-form text



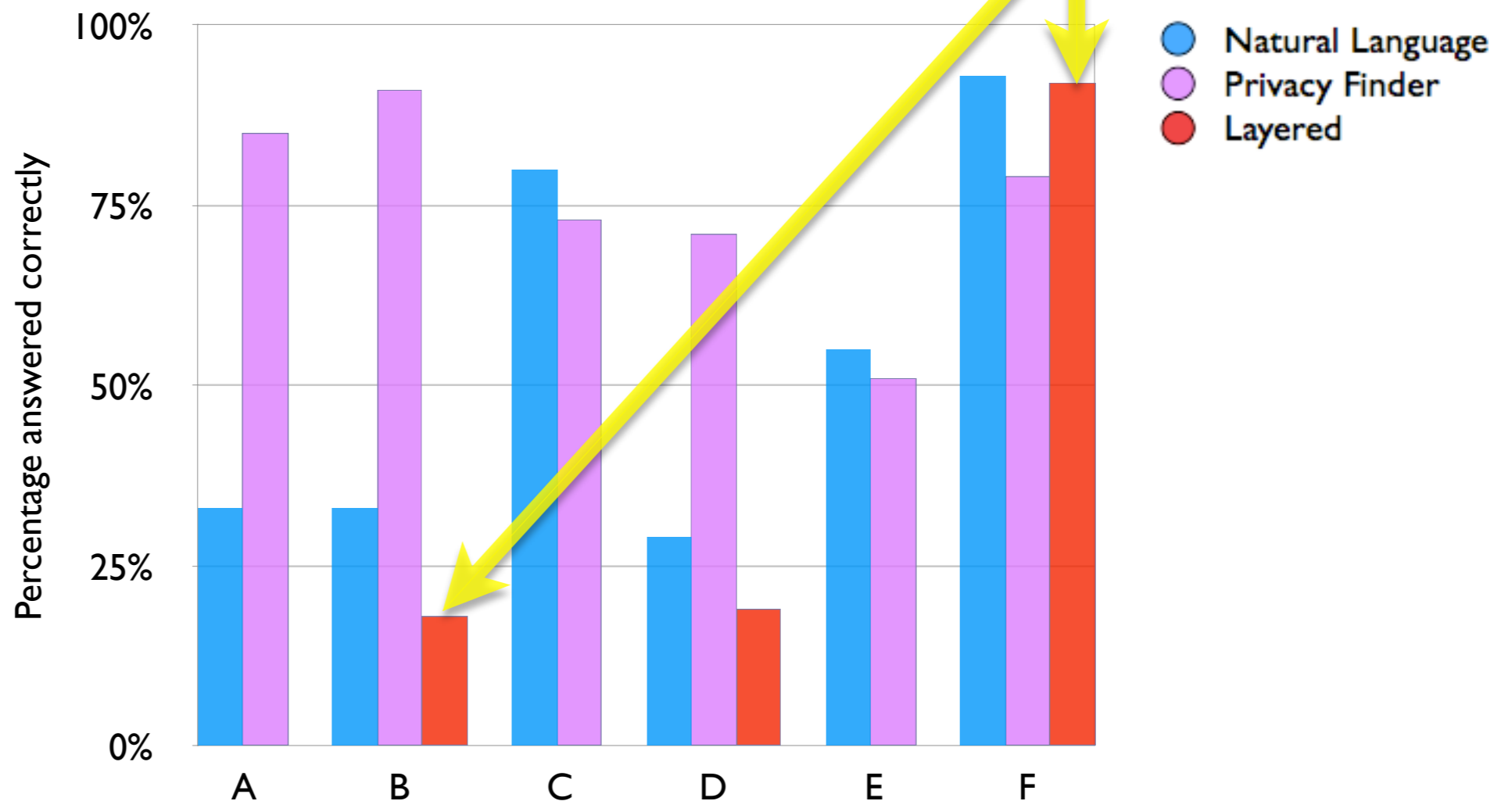
link to a webform... to remove yourself from Acme's email marketing list

- NL from 93% (F) to 33% (A)
 - Required finding a link in 13 pages
- PF from 91% (B) to 51% (E)
 - F PF (79%) same practices as E PF (51%), difference in free-form text
- F layered (92%) same text as F PF (79%)



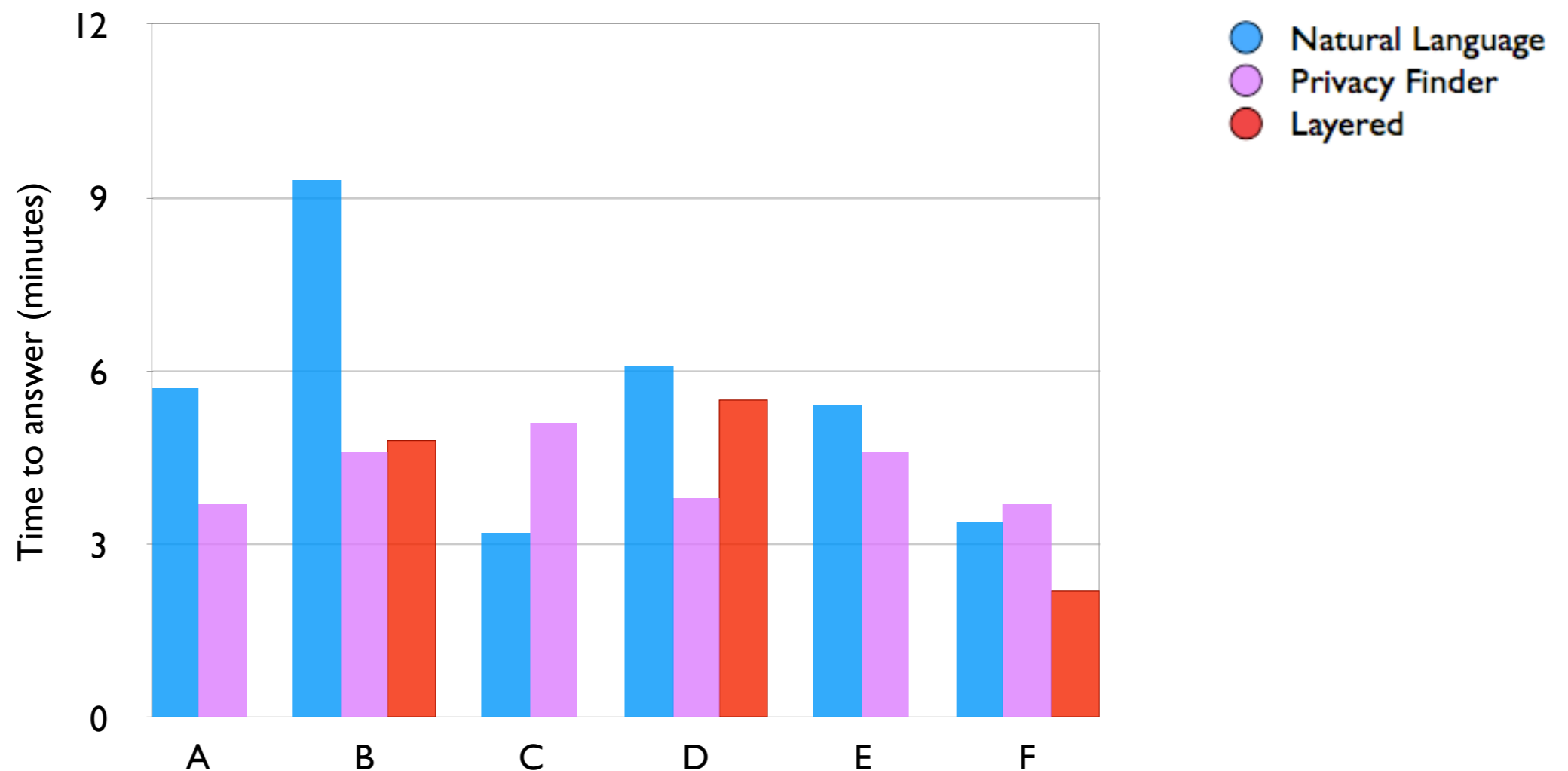
link to a webform... to remove yourself from Acme's email marketing list

- **NL** from 93% (F) to 33% (A)
 - Required finding a link in 13 pages
- **PF** from 91% (B) to 51% (E)
 - F **PF** (79%) same practices as E **PF** (51%), difference in free-form text
- F **layered** (92%) same text as F **PF** (79%)
- **Layered** from 92% (F) to 18% (B)
 - B **layered** (18%) required clicking link to see what it did



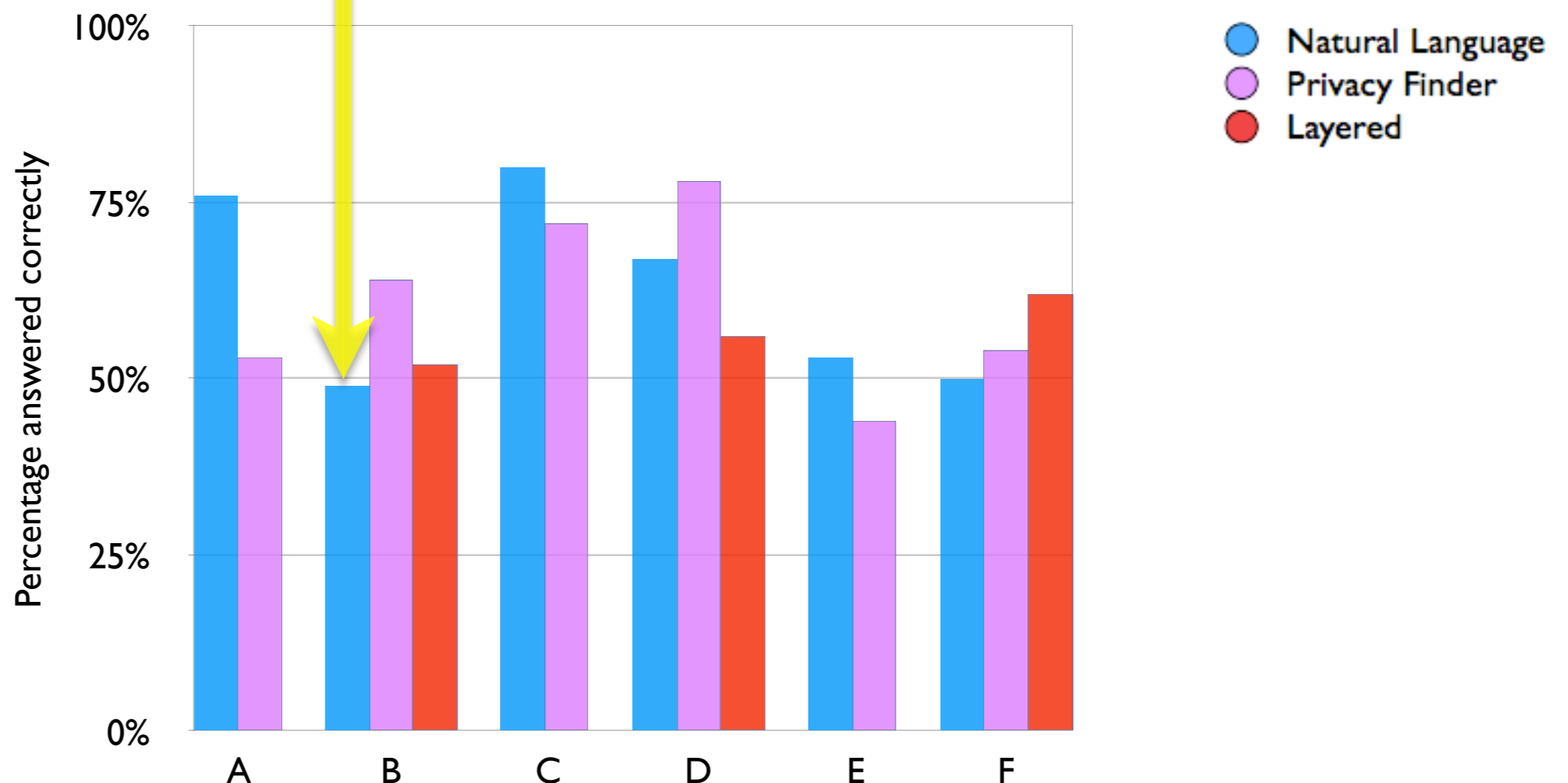
link to a webform... to remove yourself from Acme's email marketing list

- Expected longer times for longer policies
- Instead, main factor was: no link took longer
- Re-reading rather than just reading to end of policy
- **Layered** (4.0) and **PF** (4.2) faster than **NL** (5.4,) but accuracy all over the map



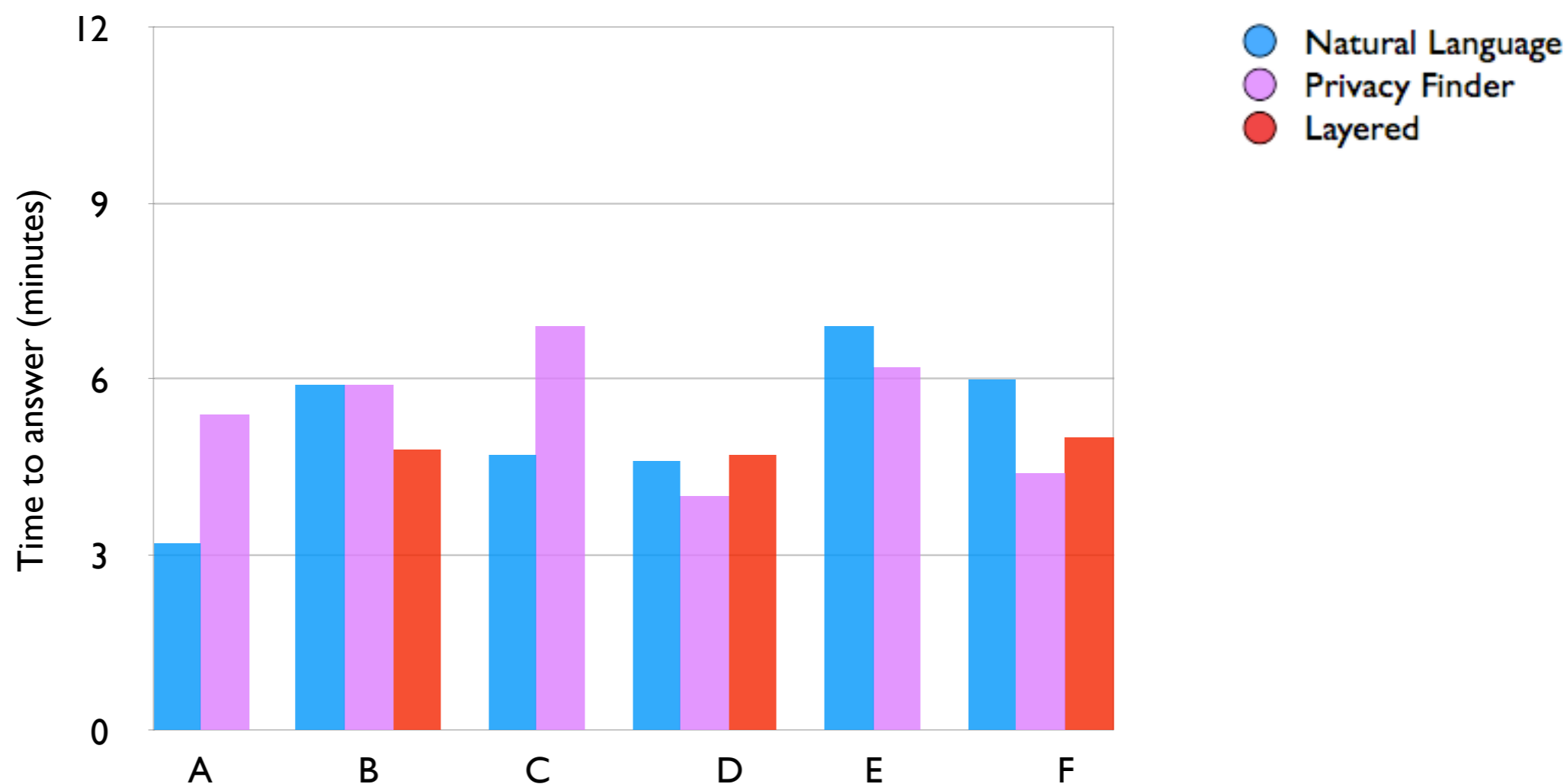
share email address with co. that might put you on email marketing list (with or w/out consent)?

- Overall accuracy only 60%
- Requires inferences, ex B NL:
“We may provide your contact info & other personal data to trusted third parties to provide information on products and services that may be of interest to you.”
- No pattern based on readability for NL
- No significance for formats



share email address with co. that might put you on email marketing list (with or w/out consent)?

- No significant differences for company or format
- Longer times (5.2 minutes) indicate this was a more difficult question to answer



use phone # for telemarketing?

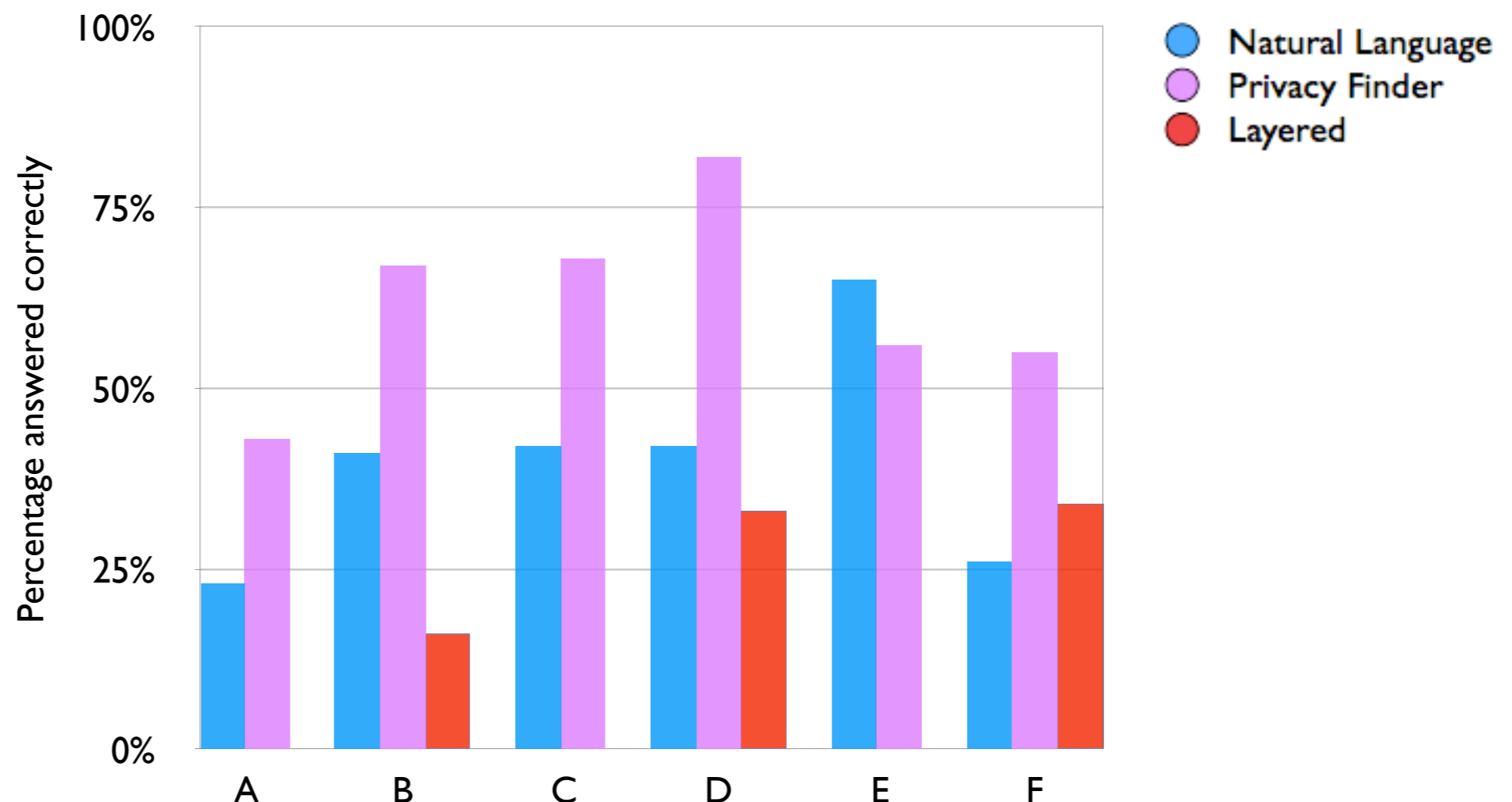
- Hard question, jigsaw puzzle

“The information you provide to Acme on certain Acme Web sites may also be used by Acme and selected third parties for marketing purposes.” *plus* another section on phone #s

- Layered accuracy only 28%

- PF only format that requires telemarketing notice

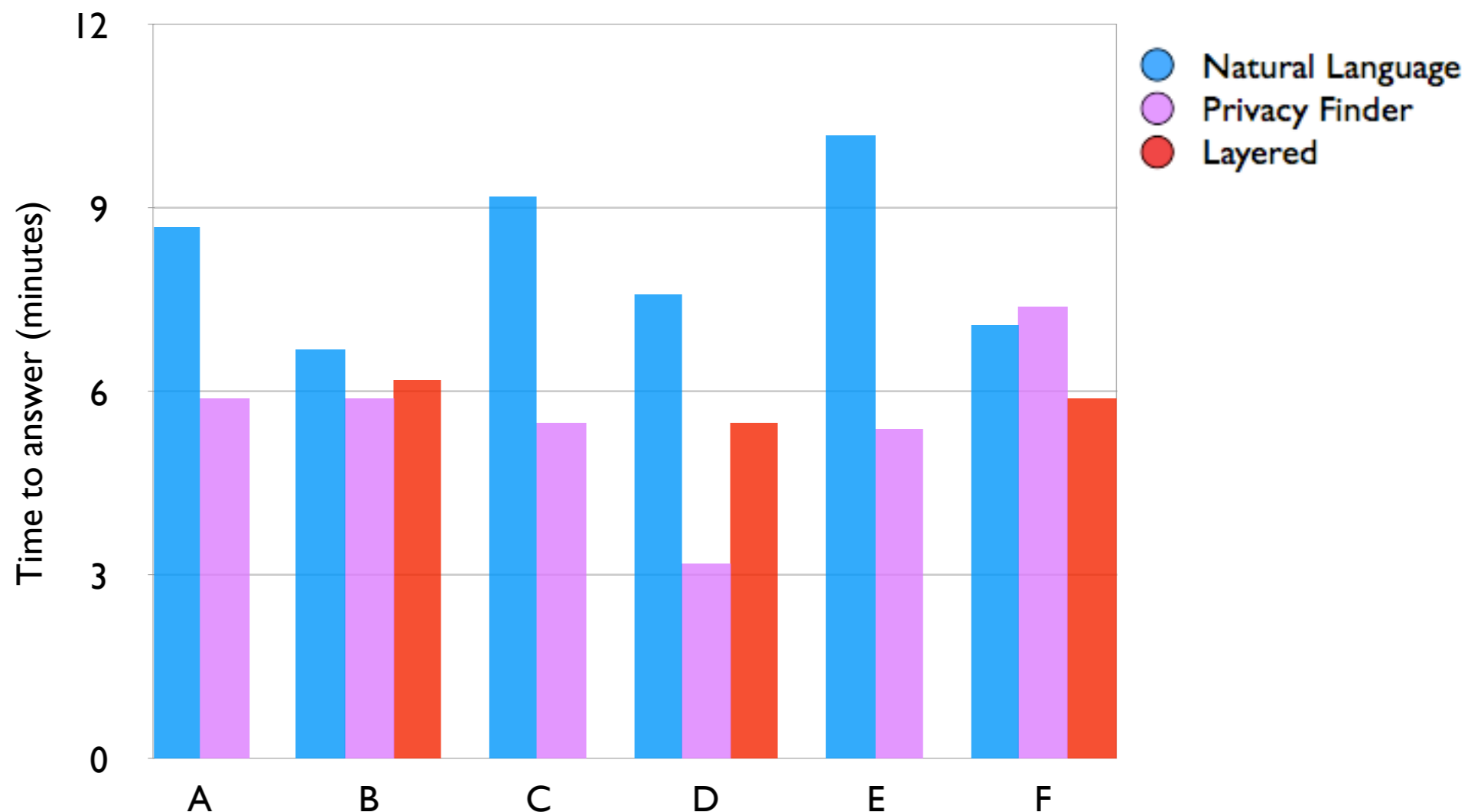
- PF supported more accurate answers (61%) in contrast to NL (39%)



use phone # for telemarketing?

■ Not significant for company, only format

■ Layered & Privacy Finder faster (5 min) than Natural Language (8.2 min)



Psychological Acceptability

- People do not use what they do not like
- Asked eight questions on a seven-point Likert scale
 - Strongly agree to strongly disagree with statements



Psychological Acceptability

- People do not use what they do not like
- Asked eight questions on a seven-point Likert scale
 - Strongly agree to strongly disagree with statements
- Summary of results:
 - Privacy policies of all formats and from all companies were disliked
 - Many results not significant, those that were had small effect sizes
 - Layered slightly better liked
 - Privacy Finder slightly more trusted



Discussion

- All formats unsatisfactory
 - Low comprehension for synthesis questions
 - Participants disliked all
- Better readability for NL did not improve comprehension
- Larger than expected range within standardized formats
 - Same practices, different results
 - Authors have much leeway
- Current standardized formats not very different from NL
 - PF better for complexity if topic part of P3P specification
 - Layered faster yet less accurate: link hides information
- Policy implications:
 - Test new formats first
 - We do not suggest regulation requiring standardized formats
 - Standardization remains a promising idea — can we do better in future revisions?



Nutrition Label for Privacy

types of information	how we use your information				who we share your information with	
	provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information	!	opt out	opt out		opt in	
cookies	!	opt out	opt out		opt in	
demographic information						
financial information						
health information						
preferences	!	opt out	opt out		opt in	!
purchasing information	!	opt out	opt out		opt in	
social security number & gov't ID	!					
your activity on this site	!	opt out	opt out		opt in	!
your location						



Now What?



A Few Policy Choices

- Do nothing
- Modify self-regulation
- Try a new approach
- Everything all at once



Do Nothing

■ Some views of proponents

- Need more time for self-regulation to work
- No need for action because at least one of:
 - Privacy is bad
 - Status quo is fine
 - Privacy is dead
 - Just wait for older generation to die off

■ Some views of opponents

- Causing harm now especially to the vulnerable
- Public is outraged when they understand practices
- Self-regulation is not working
- Losing potential customers
- Privacy is a basic right deserving full protection



Modify Self-Regulation

■ Some views of proponents

- Companies innovate when *threatened* with regulation
- Privacy Enhancing Tech
 - Reinvent P3P
 - Reinvent privacy seals
 - Opt out cookies, TACO
- Publish sample policies
- Mandate better formats
- Redefine success: policies are not to be widely read

■ Some views of opponents

- Privacy protections should not be a user burden
- People mistakenly believe “privacy policy” means they are protected
- Trained users out of clicking the privacy policy link
- Better privacy policies necessary but not sufficient
- Privacy is not a commodity



Try a New Approach

■ Some views of proponents

- Legislation from Congress
- Regulation from the FTC
- First rounds may be toothless, can amend later
- Right to anonymous speech is constitutionally protected
- General opposition to industry self-regulation
- Have tried everything else

■ Some views of opponents

- Government will only harm
- Unconstitutional for free speech; FTC lacks authority
- Quantifiable economic harms v. uncertain benefits
- Uncertain on the optimal level of privacy
- Internet too young
- Industry too strong
- Creates a floor or a ceiling?



Everything All At Once

New regulation

plus industry associations

plus standards bodies

plus privacy enhancing technologies

plus privacy reducing technologies

plus privacy principles

plus human rights treaties

plus social changes...



Photo by Catherine Trigg



Cylab Usable Privacy and Security Laboratory

<http://cups.cs.cmu.edu/>

Carnegie Mellon

